CN2600 Series Dual-LAN Terminal Server User's Manual

Third Edition, November 2010

www.moxa.com/product

© 2010 Moxa Inc., all rights reserved.
Reproduction without permission is prohibited.

CN2600 Series Dual-LAN Terminal Server User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2010 Moxa Inc.
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

MOXA is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information
www.moxa.com/support

Moxa Americas:
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office):
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe:
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific:
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

Chapter 1 **Introduction....1-1**

Product Features.... 1-2
Hardware.... 1-2
Software.... 1-2
Package Checklist.... 1-2
Front Panel.... 1-3
Rear Panel.... 1-4
Bottom Label.... 1-5

Chapter 2 **Hardware Installation....2-1**

Desktop.... 2-2
Rackmount.... 2-2
Wiring Requirements.... 2-2
Connecting the CN2600-8/16's Power.... 2-3
Connecting to the Network.... 2-3
Connecting to a Serial Device.... 2-3
Connecting to the Console Port.... 2-3
Adjustable Pull High/Low Resistors for the RS-485 Port.... 2-4

Chapter 3 **Initial IP Address Configuration....3-1**

Static and Dynamic IP Addresses.... 3-2
Factory Default IP Address.... 3-2
Configuration Options.... 3-2
Terminal Server Search Utility.... 3-2
Web Console.... 3-2
LCM Console/Front Panel.... 3-2
ARP.... 3-3
Telnet Console.... 3-4
Serial Console.... 3-9

Chapter 4 **Serial Port Operation Modes....4-1**

Overview.... 4-2
Device Control Applications.... 4-2
Real COM Mode.... 4-3
RFC2217 Mode.... 4-3
Socket Applications.... 4-3
TCP Server Mode.... 4-4
TCP Client Mode.... 4-4
UDP Mode.... 4-5
Redundant COM.... 4-5
Dual-host Redundant Data Acquisition System (DRDAS).... 4-6
Terminal Applications.... 4-8
Terminal ASCII Mode.... 4-8
Terminal BIN Mode.... 4-8
Reverse Terminal Applications.... 4-9
Reverse Telnet.... 4-9
Dial In/Out Modes.... 4-10
Disabled Mode.... 4-10

Chapter 5 **Configuration with the Web Console.....5-1**
Using Your Web Browser..... 5-2
Browser Cookie Settings..... 5-2
Trusted Site Settings..... 5-3
Opening the Web Console..... 5-4
Web Console Navigation..... 5-5
Basic Settings..... 5-6
Server Settings..... 5-6
Time Settings..... 5-6
Network Settings..... 5-7
Basic Network Settings..... 5-7
Advanced Network Settings..... 5-9
Configuring the Route Table..... 5-10

Chapter 6 **Configuring Serial Port Operation Modes.....6-1**
Port Setting Basics..... 6-2
Device Control Applications..... 6-3
Real COM Mode..... 6-3
RFC2217 Mode..... 6-5
Socket Applications..... 6-7
TCP Server Mode..... 6-7
TCP Client Mode..... 6-9
UDP Mode..... 6-12
Redundant COM..... 6-14
DRDAS..... 6-16
DRDAS Real COM..... 6-16
DRDAS TCP Server..... 6-18
Terminal Applications..... 6-20
Terminal ASCII (TERM_ASC)..... 6-20
Terminal BIN (TERM_BIN)..... 6-22
Reverse Terminal..... 6-23
Dial In/Out Applications..... 6-24
PPP Mode..... 6-24
PPPD Mode..... 6-25
SLIP Mode..... 6-26
SLIPD Mode..... 6-27
Dynamic Mode..... 6-28
Disabled Mode..... 6-28

Chapter 7 **Additional Serial Port Settings.....7-1**
Port Communication Parameters..... 7-2
Serial Parameters..... 7-2
Port Data Buffering/Log..... 7-3
Port Modem Settings..... 7-3
Welcome Message..... 7-4

Chapter 8 **System Management Settings.....8-1**
Misc. Network Settings..... 8-2
Accessible IP List..... 8-2
SNMP Agent Settings..... 8-3
DDNS..... 8-4

Host Table 8-4
User Table 8-5
Authentication Server 8-6
System Log Settings 8-6
Auto Warning Settings 8-7
Event Settings 8-7
Serial Event Settings 8-8
E-mail Alert 8-9
SNMP Trap 8-10
Maintenance 8-10
Console Setting 8-10
Ping 8-11
Firmware Upgrade 8-11
Configurating Import/Export 8-12
Load Factory Defaults 8-13
Change Password 8-13
Certificate 8-14
Ethernet SSL Certificate Import 8-14
Certificate/Key Delete 8-14
System Monitoring 8-15
Serial to Network Connections 8-15
Serial Port Status 8-15
Serial Port Error Count 8-16
Serial Port Settings 8-16
Network Connections 8-16
Network Statistics 8-17
Serial Data Log 8-17
System Log 8-18
Routing 8-18
Save Configuration 8-19
Restart 8-19
Restart System 8-19
Restart Ports 8-20

Chapter 9 Software Installation/Configuration 9-1

NPort Search Utility 9-2
Installing NPort Search Utility 9-2
Configuring NPort Search Utility 9-4
Windows Driver Manager 9-7
Installing NPort Windows Driver Manager 9-7
Using NPort Windows Driver Manager 9-10
Windows Monitor Utility 9-17
Installing the NPort Monitor Utility 9-17
Using the NPort Monitor Utility 9-20
Linux Real TTY Drivers 9-22
Basic Procedures 9-22
Hardware Setup 9-22
Installing Linux Real TTY Driver Files 9-22
Mapping TTY Ports 9-23
Removing Mapped TTY Ports 9-23
Removing Linux Driver Files 9-24

The UNIX Fixed TTY Driver 9-24
Installing the UNIX Driver 9-24
Configuring the UNIX Driver 9-25

Appendix A Pinouts and Cable Wiring A-1
Port Pinout Diagrams A-2
RS-232/422/485 (Male DB9) Pinouts A-2
RS-232 (Male DB9) Pinouts A-2
RS-232 (Male RJ45) Pinouts A-3
RS-232/422/485 (Male RJ45) Pinouts A-3
Cable Wiring Diagrams A-4
Ethernet Cables A-4
Serial Cables (RS-232) A-4
Serial Cables (RS-422/4-Wire RS-485) A-6
Serial Cables (2-Wire RS-485) A-7
Pin Assignments for DB9 and DB25 Connectors A-8

Appendix B SNMP Agent with MIB II B-1

Appendix C Dynamic Domain Name Server C-1
Overview C-1
Configuration C-2

Appendix D Well Known Port Numbers D-1

Appendix E RADIUS Server E-1
What is RADIUS? E-2
Definition E-2
Client/Server Architecture E-2
Setting up the CN2600 ..... E-2
Setting up the RADIUS Server IP Address E-2
Serial Port Configuration E-3
Setting up UNIX Hosts E-3
Setting up Windows NT Hosts E-4
Setting up Windows 2000 Hosts E-6
Setting up Windows 2003 Hosts E-9

1

Introduction

Moxa's CN2600 series of dual-LAN terminal servers is available in models with 8 or 16 RS-232 or RS-232/422/485 ports, and all models come with two 10/100 Mbps Ethernet LAN ports. The CN2600 dual-LAN terminal servers are used to connect terminals, modems, printers, and other asynchronous serial devices to LAN hosts. The CN2600 dual-LAN terminal servers comply with TCP/IP and IEEE 802.3 specifications using standard Ethernet 10/100BaseT and twisted pair 10/100BaseTX cable as the data transmission medium.

NOTE: In this manual, we often refer to all terminal servers in the CN2600 series collectively as the CN2600.

NOTE:The wide temperature model does not have an LCM Display panel and push buttons. The LCM description in this manual applies only to standard temperature models.

The following topics are covered in this chapter:

- **Product Features**
  - Hardware
  - Software
- **Package Checklist**
- **Front Panel**
- **Rear Panel**
- **Bottom Label**

Product Features

Hardware

- Dual LAN ports (auto-detecting 10/100 Mbps Ethernet)
- 8 MB RAM, 16 MB Flash ROM
- Tx/Rx LEDs for each serial port
- System Status LEDs
- Ethernet Status LEDs
- 8 or 16 RJ45 RS-232 serial ports, with up to 921.6 Kbps transmission speed
- 2 KV Serial Line Protection (for isolation models)

Software

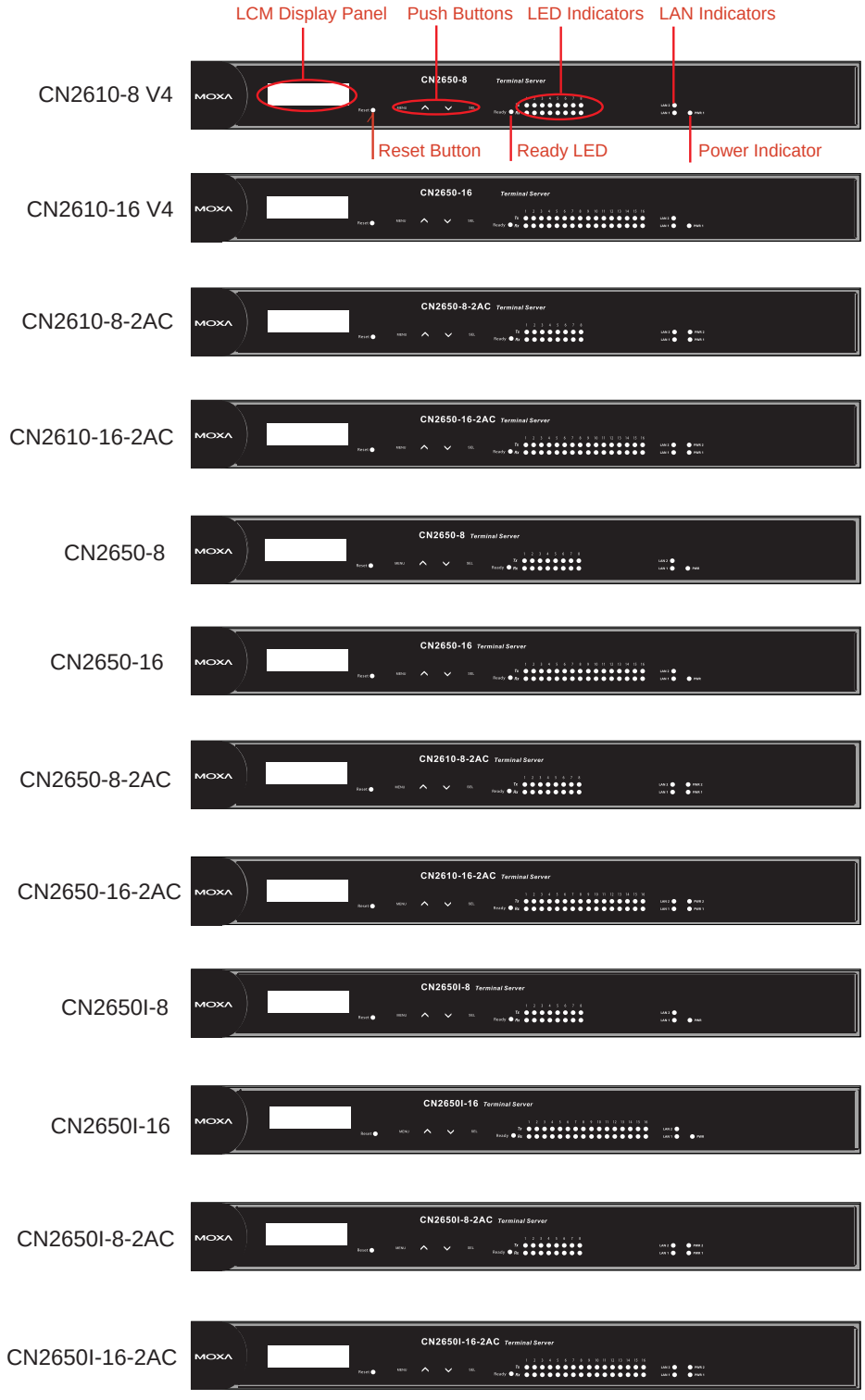
- ASCII/Binary terminal modes with up to 8 Telnet and Rlogin sessions
- Point to Point Protocol (PPP and PPPD)
- Serial Line Internet Protocols (SLIP and SLIPD)
- Dynamic auto-recognition of Terminal, SLIP, or PPP
- Dial-on-demand, Dial-out
- CN2600 series Terminal Server Proprietary Protocol (ASPP) for TCP/IP socket programming
- RAW mode for transparent data transmission
- Reverse Telnet
- SNMP Agent for network management
- Network protocols: TCP/IP, UDP, ICMP, NetBEUI, DHCP
- Application protocols: Telnet, Rlogin, Rtelnet, RAW TCP, RAW UDP, WINS, DRDAS™, DNS, Multi-Host
- Security protocols: RADIUS, Dial-back, PAP, CHAP, Local user/password
- Real COM port drivers (Windows 95/98/ME/NT/2000, Windows XP/2003/Vista/2008/7 x86/x64)
- Real TTY drivers (Linux kernel 2.4.x, 2.6.x)
- **Fixed TTY Drivers:** SCO Unix, SCO OpenServer, UnixWare 7, UnixWare 2.1, SVR 4.2, QNX 4.25, QNX 6, Solaris 10, FreeBSD, AIX 5.x
- Static Routing, RIP I/II protocols
- Windows-like administrative CONSOLE utility from a fixed console port, or by Telnet from a networked host
- Password protection and extensive user verification functions
- Easy firmware upgrade via Flash ROM

Package Checklist

All CN2600 dual-LAN terminal servers are shipped with the following items:

- CN2600 dual-LAN terminal server
- AC power cord
- Document and Software CD-ROM
- Quick Installation Guide (English and Simplified Chinese versions)
- RJ45 Loopback Tester
- Product Warranty Statement
- Rackmount Kit (includes 2 brackets and 8 screws)
- Desktop Kit (includes 4 pads)

Front Panel


LCM Display Panel
Push Buttons
LED Indicators
LAN Indicators
CN2610-8 V4
CN2650-8
Terminal Server
Reset Button
Ready LED
Power Indicator
CN2610-16 V4
CN2650-16
CN2650-8-2AC
CN2610-8-2AC
CN2650-16-2AC
CN2610-16-2AC
CN2650-8
CN2650-16
CN2610-8-2AC
CN2650-8-2AC
CN2610-16-2AC
CN2650-16-2AC
CN2650I-8
CN2650I-16
CN2650I-8-2AC
CN2650I-16-2AC

Buttons and LEDs

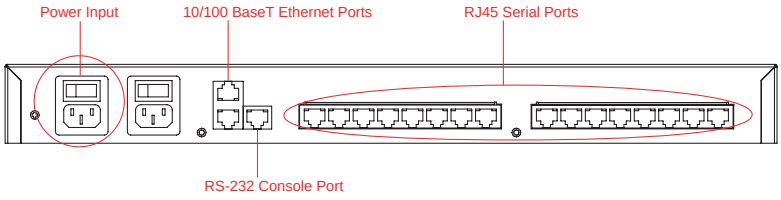
Item	Description
Reset Button	Press the Reset button for 5 seconds to load factory defaults. The CN2600 will beep twice when the configuration has been reset.
Push Buttons	Used for configuring the IP address and other parameters.

(LEDs)

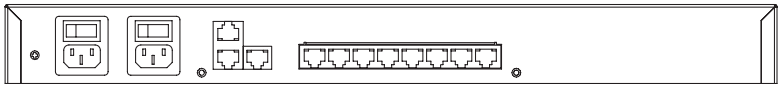
Ready	Red	Indicates that the CN2600 is receiving power
	Green	Indicates that the CN2600's OS is ready
Tx	Green	Indicates serial port transmission
Rx	Yellow	Indicates serial port reception
LAN 1, LAN 2	Green	Ethernet link connection
	Off	Ethernet cable is disconnected
PWR 1, PWR 2	Red	Power connection
	Off	Power cable is disconnected

Rear Panel

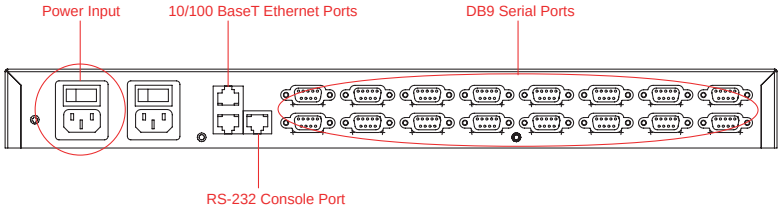
CN2610-16-2AC
CN2650-16-2AC



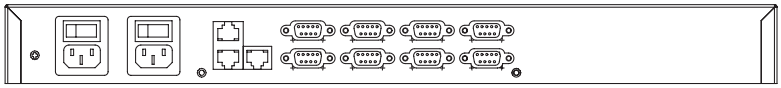
CN2610-8-2AC
CN2650-8-2AC



CN2650I-16-2AC



CN2650I-8-2AC



Socket / Port	Description
AC Power Input	Automatic detection of 100-240V, 47-63 Hz AC power supply
Power On/Off Switch	I indicates power on; O indicates power off (AC models only)
Console	8-pin RJ45 RS-232 port for console terminal connection
LAN 1	8-pin RJ45 auto-detectable 10/100 Mbps UTP port
LAN 2	8-pin RJ45 auto-detectable 10/100 Mbps UTP port
Serial Ports	8 or 16 8-pin RJ45 or DB9 ports for DCE modem-type connections

Bottom Label

The server's serial number and MAC address are printed on a label fixed to the bottom of the server. The CN2600 has 2 LAN ports, each with its own MAC address. The MAC address is the unique hardware Ethernet address used to identify a network hardware product. Write each of the two MAC addresses in the space provided below for future reference.

LAN 1 MAC address:_____

LAN 2 MAC address:_____

2

Hardware Installation

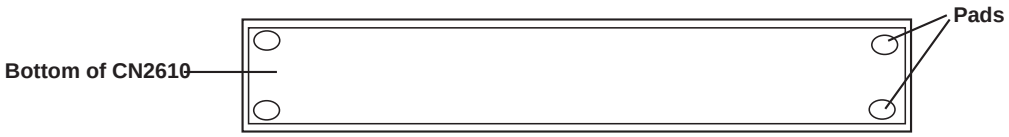
This chapter includes instructions on where and how to install the CN2600 dual-LAN terminal server. Both basic and advanced software configuration instructions are given.

The following topics are covered in this chapter:

- **Desktop**
- **Rackmount**
- **Wiring Requirements**
- **Connecting the CN2600-8/16's Power**
- **Connecting to the Network**
- **Connecting to a Serial Device**
- **Connecting to the Console Port**
- **Adjustable Pull High/Low Resistors for the RS-485 Port**

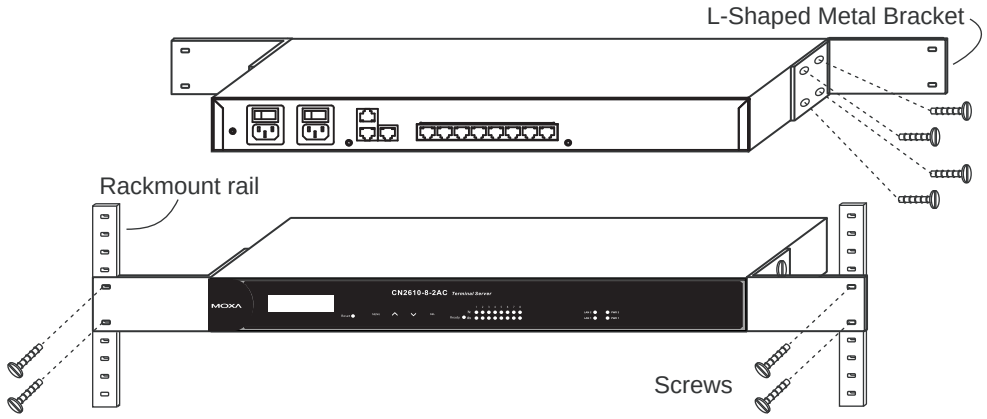
Desktop

Place your CN2600 on a clean, flat, well-ventilated desktop. For better ventilation, attach the 4 pads from the desktop kit to the bottom of the unit, and leave some space between the CN2600 and other equipment. Do not place equipment or objects on top of the unit, as this might damage the server.



Rackmount

The CN2600 is designed to be mounted on a standard 19-inch rack. Use the enclosed pair of L-shaped metal brackets and screws to fasten your CN2600 to the rack cabinet. Each L-shaped bracket has 6 holes, leaving two outer or inner holes available for other uses. You have two options. You can lock either the front or rear panel of the CN2600 to the front of the rack. Locking the front panel is shown in the following figure.



Wiring Requirements

ATTENTION

Safety First!

Be sure to disconnect the power cord before installing and/or wiring your CN2600.

Wiring Caution!

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.

If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

Temperature Caution!

Be careful when handling the CN2600. When plugged in, the CN2600's internal components generate heat, and consequently the board may feel hot to the touch.

You should also observe the following common wiring rules:

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.

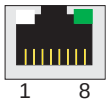
  NOTE: Do not run signal or communication wiring and power wiring in the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
- You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- Keep input wiring and output wiring separate.
- Where necessary, it is strongly advised that you label wiring to all devices in the system.

Connecting the CN2600-8/16's Power

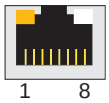
Connect the CN2600's 100-240 VAC power line to its AC connector. If the power is properly supplied, the "Ready" LED will show a solid red color until the system is ready, at which time the color changes to green.

Connecting to the Network

Connect one end of the Ethernet cable to the CN2600's 10/100M Ethernet port and the other end of the cable to the Ethernet network. There are 2 LED indicators located on the top left and right corners of the Ethernet connector. If the cable is properly connected, the CN2600 will indicate a valid connection to the Ethernet in the following ways:



The top right corner LED indicator maintains a solid green color when the cable is properly connected to a 100 Mbps Ethernet network.



The top left corner LED indicator maintains a solid orange color when the cable is properly connected to a 10 Mbps Ethernet network.

Connecting to a Serial Device

Use appropriately wired serial data cables to connect serial devices to the CN2600's serial ports.

Connecting to the Console Port

A console is a combination of keyboard and monitor that is used to configure settings and monitor the status of your system. The console port can be used if a network is unavailable, or you do not know the CN2600's IP address. To connect to the console port, use a PC running UNIX, or a PC with terminal emulation software (e.g., HyperTerminal or PComm by Moxa; parameter settings are: baudrate = 115200 bps, parity check = None, data bits = 8, stop bits = 1, terminal type = VT100). Use an RJ45-to-DB25 or RJ45-to-DB9 cable to connect the terminal to the console port.

Adjustable Pull High/Low Resistors for the RS-485 Port

In some critical environments, you may need to add termination resistors to prevent the reflection of serial signals. When using termination resistors, it is important to set the pull high/low resistors correctly so that the electrical signal is not corrupted. The CN2600 uses jumper settings or DIP switches to set the pull high/low resistor values for each serial port.

To set the pull high/low resistors to 150 KΩ, make sure both of the assigned DIP switches are in the OFF position. This is the default setting.

To set the pull high/low resistors to 1 KΩ, make sure both of the assigned DIP switches are in the ON position.

ATTENTION

Do not use the 1 KΩ setting on the CN2610 when using the RS-232 interface. Doing so will degrade the RS-232 signals and shorten the maximum allowed communication distance.

3

Initial IP Address Configuration

When setting up the CN2600 for the first time, the first thing you should do is configure its IP address. This chapter introduces the different methods that can be used. Please refer to Chapter 8, System Management Settings, for more details about network settings.

The following topics are covered in this chapter:

- **Static and Dynamic IP Addresses**
- **Factory Default IP Address**
- **Configuration Options**
  - Terminal Server Search Utility
  - Web Console
  - LCM Console/Front Panel
  - ARP
  - Telnet Console
  - Serial Console

Static and Dynamic IP Addresses

Determine whether your CN2600 needs to use a static IP or dynamic IP address (either DHCP or BOOTP/PPPoE application).

- ***If your CN2600 terminal server is used in a static IP environment***, you will assign a specific IP address using one of the tools described in this chapter.
- ***If your CN2600 terminal server is used in a dynamic IP environment***, the IP address will be assigned automatically from over the network. In this case, set the IP configuration mode to DHCP, DHCP/BOOTP, BOOTP, or PPPoE.

ATTENTION

Consult your network administrator on how to reserve a fixed IP address for your CN2600 in the MAC-IP mapping table when using a DHCP Server or BOOTP Server. For most applications, you should assign a fixed IP address to your CN2600.

Factory Default IP Address

The CN2600 is configured with the following default private IP addresses:

192.168.126.254 and 192.168.127.254

Note that IP addresses that begin with "192.168" are referred to as private IP addresses. Devices configured with a private IP address are not directly accessible from a public network. For example, you would not be able to ping a device with a private IP address from an outside Internet connection. If your application requires sending data over a public network, such as the Internet, your CN2600 will need a valid public IP address, which can be leased from a local ISP.

Configuration Options

Terminal Server Search Utility

You may configure your CN2600 with the bundled NPort Search Utility for Windows. Please refer to Chapter 9 Software Installation/Configuration, for details on how to install and use Terminal Server Search Utility.

Web Console

You may configure your CN2600 using a standard web browser. Please refer to Chapter 5 Configuraton with the Web console, for details on how to access and use the CN2600 web console.

LCM Console/Front Panel

The CN2600 only gives you the option to configure some settings through the front panel, also known as the LCM (Liquid Crystal Module) console. The LCM console can be configured for read-only or writeable access. Read-only access allows settings to be viewed but not changed. Factory default settings are for writeable access, where configuration is allowed through the LCM console.

NOTE The wide temperature model does not have an LCM Display panel and push buttons. The LCM description below applies only to standard temperature models.

ATTENTION

If a password has been enabled for the CN2600 console and the LCM console is configured for writeable status, the LCM console will require you to enter the password before allowing you access. The password will not be required if the LCM console is configured for read-only access.

The **MENU** button activates the main menu. It is also used to cancel a selection and return to a previous menu.

The **UP** and **DOWN** buttons navigate between available options.

The **SEL** button confirms a selection or enters a submenu.

The IP environment (Static, DHCP, PPPoE, etc.) is configured under **Main Menu → Network setting → IP config**. The IP address is configured under **Main Menu → Network setting → IP address**. After the address has been entered, you will need to restart the CN2600 under **Main Menu → Save/Restart**.

The following instructions explain how to set the CN2600's IP address through the LCM console:

1. Press **MENU** to activate the Main Menu.
2. The first line of the display indicates the current menu and should read **Main Menu**. The second line indicates the current selection and should read **Server setting**. Use the **UP** and **DOWN** buttons to select **Network setting**. Press **SEL** to enter the **Network setting** menu.
3. In the **Network setting** menu, select **IP config**. Don't forget to press **SEL** to confirm your selection.
4. In the **IP config** menu, use the **UP** and **DOWN** buttons to select the option that matches your IP environment (static, DHCP, etc.). Press **SEL** to confirm your choice. You may also press **MENU** to cancel your selection and return to the previous submenu.
5. You should be back in the **Network setting** menu. From the **Network setting** menu, select **IP address**.
6. Use the **UP** and **DOWN** buttons to modify the digit currently selected by the blinking cursor. Press **SEL** to move to the next digit. Continue modifying the IP address until all digits have been entered. If you make a mistake, press **MENU** to cancel all changes and return to the **Network setting** menu. You cannot go back one digit.
7. Once you have finished modifying the IP address, your changes are saved but not in effect. In order for your changes to take effect, you will need to restart the CN2600. You may view and modify your changes by selecting **IP address** at the **Network setting** menu again.
8. Press the menu button to exit out of the **Network setting** menu and return to the **Main Menu**. Use the **UP** and **DOWN** buttons to select **Save/Restart** and press **SEL**. Use the **UP** and **DOWN** buttons to select **Yes** and press **SEL** to restart.

ARP

You may use the ARP (Address Resolution Protocol) command to set up an IP address for your CN2600. The ARP command tells your computer to associate the CN2600's MAC address with an IP address. Afterwards, use Telnet to access the CN2600 and its IP address will be reconfigured.

ATTENTION

In order to use the ARP setup method, both your computer and the CN2600 must be connected to the same LAN. Alternatively, you may use a cross-over Ethernet cable to connect the CN2600 directly to your computer's Ethernet card. Before executing the ARP command, your CN2600 must be configured with the factory default IP address (192.168.127.254) and your computer and the CN2600 must be on the same subnet.

To use ARP to configure the IP address, complete the following:

9. Obtain a valid IP address for your CN2600 from your network administrator.
10. Obtain your CN2600's MAC address from the label on the bottom panel.
11. Execute the arp -s command from your computer's MS-DOS prompt as follows:

    arp -s <*IP address*> <*MAC address*>

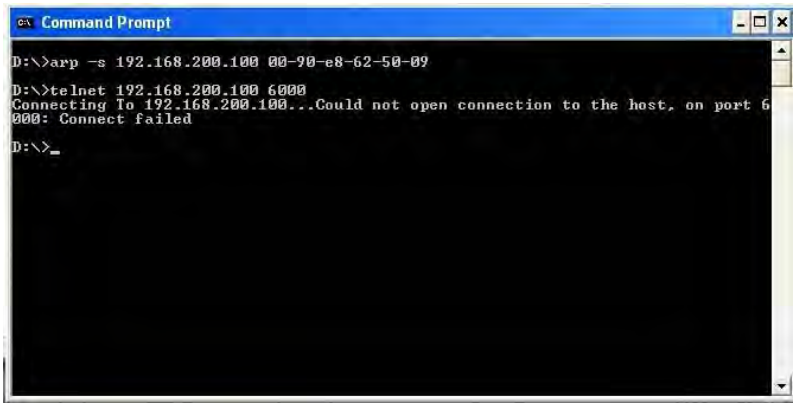
    For example,

    C:\> **arp -s 192.168.200.100 00-90-E8-04-00-11**

12. Next, execute a special Telnet command by entering the following exactly:

    telnet 192.168.200.100 6000

    When you enter this command, a **Connect failed** message will appear, as shown below.


Command Prompt
D:\>arp -s 192.168.200.100 00-90-e8-62-50-09
D:\>telnet 192.168.200.100 6000
Connecting To 192.168.200.100...Could not open connection to the host, on port 6000: Connect failed
D:\>

13. After the CN2600 reboots, its IP address will assigned to the new address and you can reconnect using Telnet to verify that the update was successful.

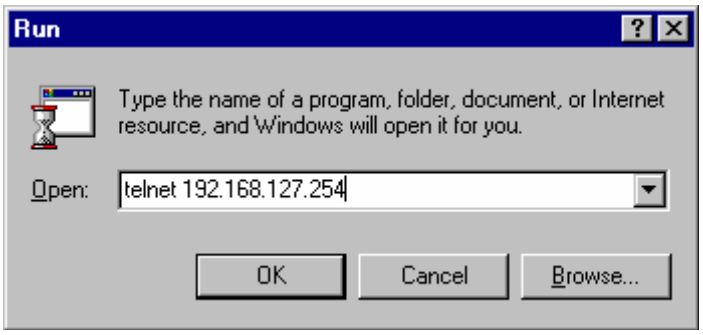
Telnet Console

Depending on how your computer and network are configured, you may find it convenient to use network access to set up your CN2600's IP address. This can be done using Telnet.

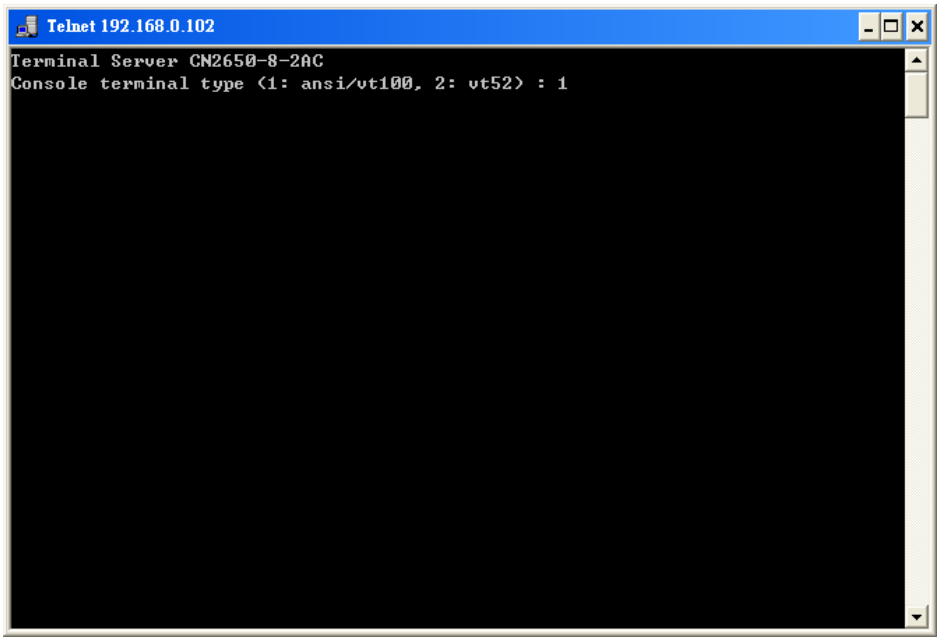
ATTENTION

Figures in this section were taken from the CN2600's Telnet console.

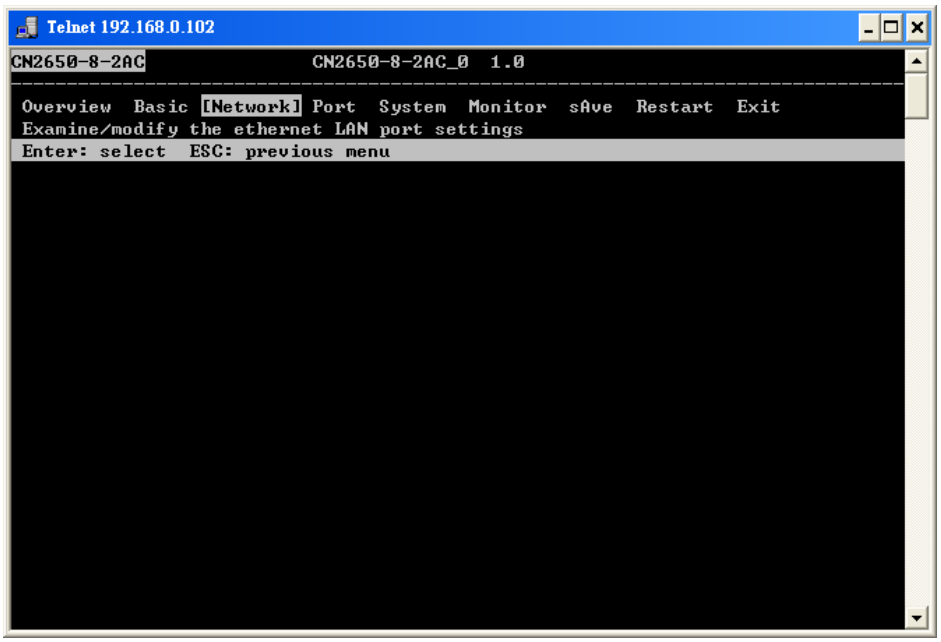
1. From the Windows desktop, select **Start → Run**, and then type **telnet 192.168.127.254** in the Run window (for LAN 1) or **telnet 192.168.126.254** (for LAN 2).
   If your IP address is different from the default setting, use your IP address instead. Click **OK**.



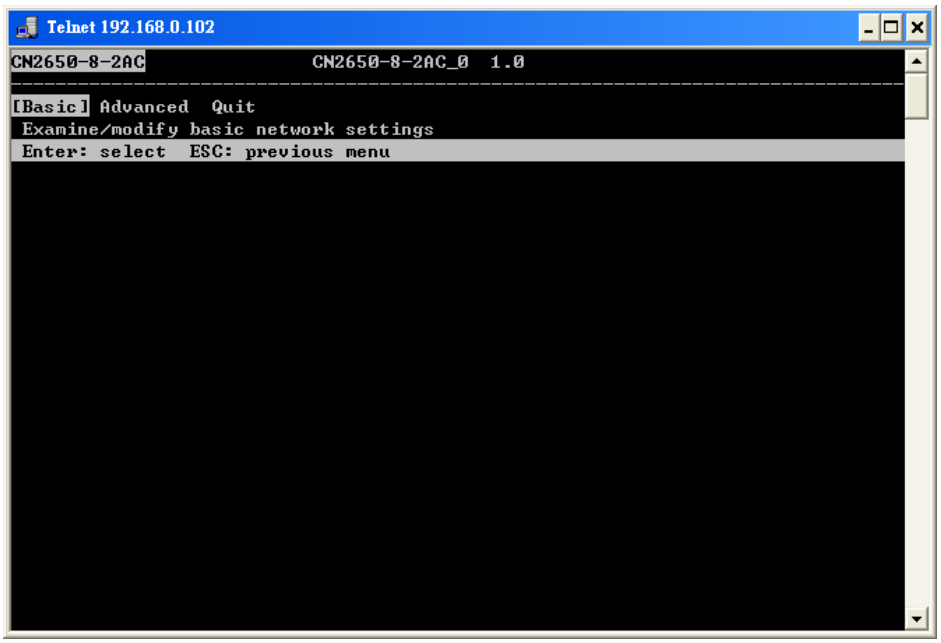
2. The console terminal type selection is displayed as shown. Enter **1** for **ansi/vt100** and press **ENTER** to continue.



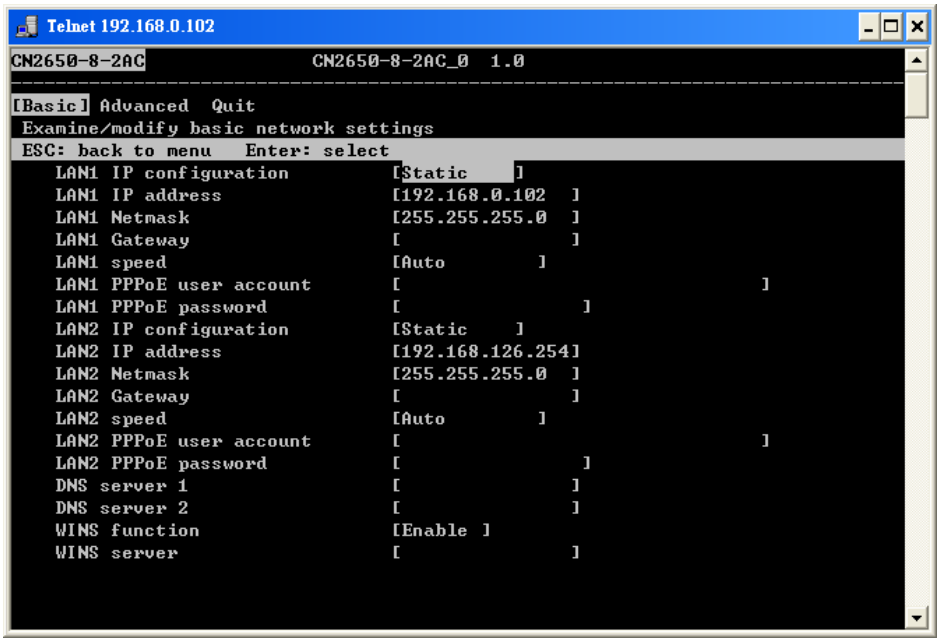
3. Press **N** or use the arrow keys to select Network, and then press **ENTER**.


Telnet 192.168.0.102
CN2650-8-2AC CN2650-8-2AC_0 1.0
Overview Basic [Network] Port System Monitor sAve Restart Exit
Examine/modify the ethernet LAN port settings
Enter: select ESC: previous menu

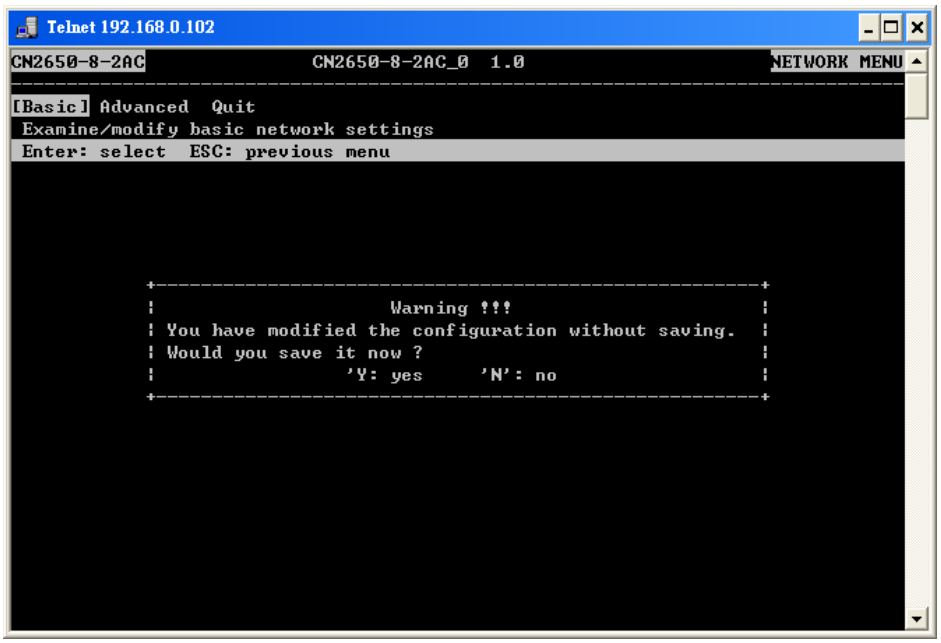
4. Press **B** or use the arrow keys to select **Basic**, and then press **ENTER**.



5. Use the arrow keys to move the cursor to **IP address**. Use the **DELETE, BACKSPACE**, or **SPACE** keys to erase the current IP address, and then type in the new IP address and press **ENTER**. Note that if you are using a dynamic IP configuration (BOOTP, SHCP, etc.), you will need to go to the **IP configuration field** and press **ENTER** to select the appropriate configuration.

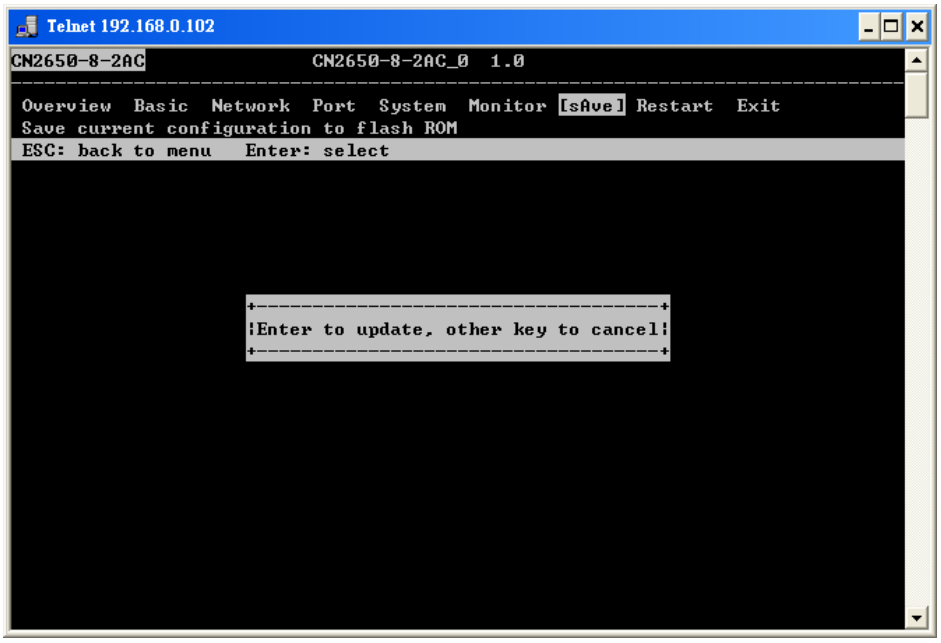

Telnet 192.168.0.102
CN2650-8-2AC CN2650-8-2AC_0 1.0
[Basic] Advanced Quit
Examine/modify basic network settings
ESC: back to menu Enter: select
LAN1 IP configuration [Static]
LAN1 IP address [192.168.0.102]
LAN1 Netmask [255.255.255.0]
LAN1 Gateway [ ]
LAN1 speed [Auto]
LAN1 PPPoE user account [ ]
LAN1 PPPoE password [ ]
LAN2 IP configuration [Static]
LAN2 IP address [192.168.126.254]
LAN2 Netmask [255.255.255.0]
LAN2 Gateway [ ]
LAN2 speed [Auto]
LAN2 PPPoE user account [ ]
LAN2 PPPoE password [ ]
DNS server 1 [ ]
DNS server 2 [ ]
WINS function [Enable]
WINS server [ ]

6. Press **ESC** twice to return to the previous page. Press **Y** to confirm the modification.

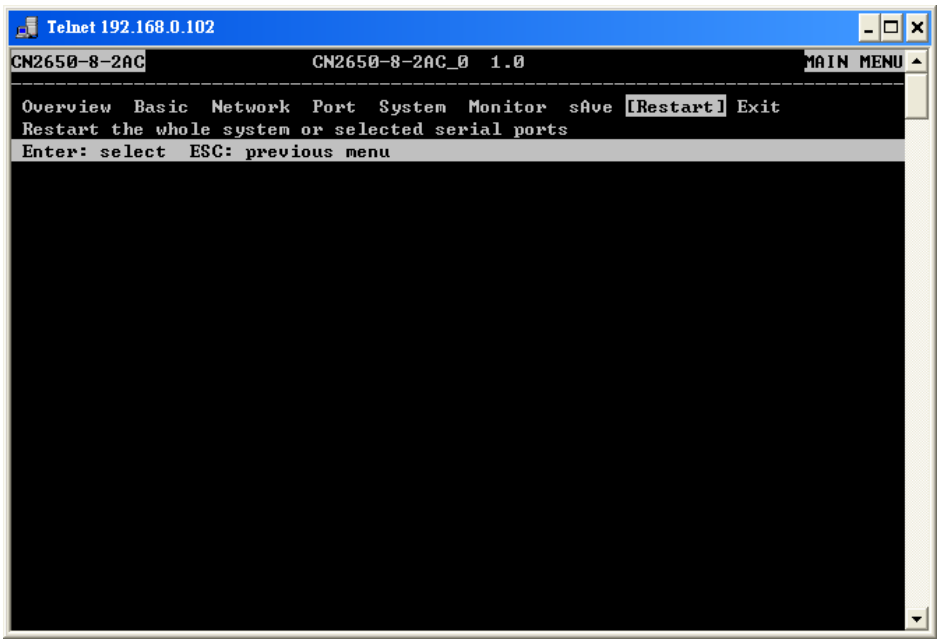

Telnet 192.168.0.102
CN2650-8-2AC CN2650-8-2AC_0 1.0 NETWORK MENU
[Basic] Advanced Quit
Examine/modify basic network settings
Enter: select ESC: previous menu
Warning !!!
You have modified the configuration without saving.
Would you save it now ?
'Y': yes 'N': no

7. Press **ESC** to return to the previous page.

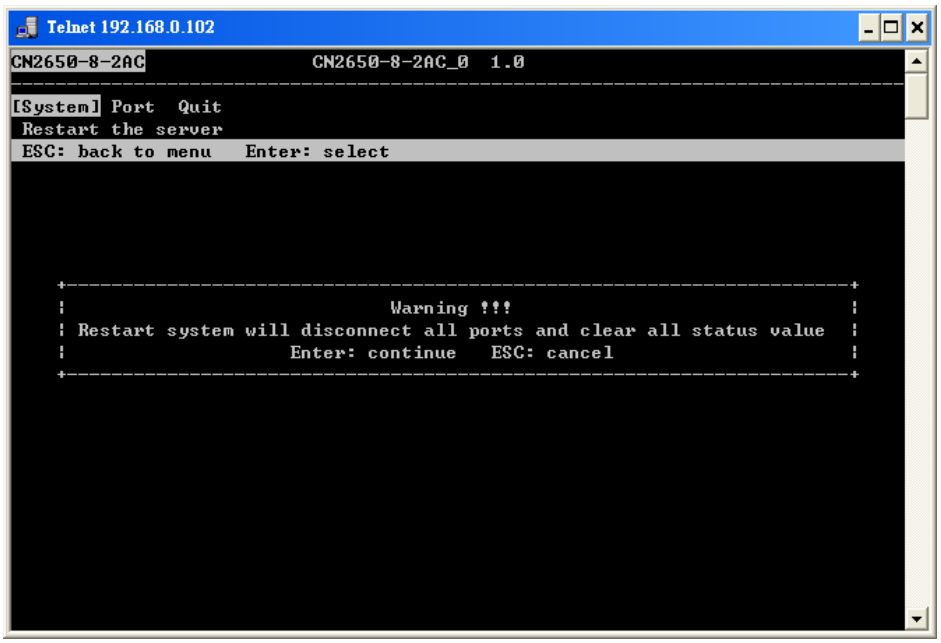
8. Press **A** or use the arrow keys to select **Save** and then press **ENTER**. Press **ENTER** again to confirm the save command.


Telnet 192.168.0.102
CN2650-8-2AC CN2650-8-2AC_0 1.0
Overview Basic Network Port System Monitor [sAve] Restart Exit
Save current configuration to flash ROM
ESC: back to menu Enter: select
+----------------------------------+
!Enter to update, other key to cancel!
+----------------------------------+

9. Press **R** or use the arrow keys to select **Restart** and then press **ENTER**.


Telnet 192.168.0.102
CN2650-8-2AC CN2650-8-2AC_0 1.0 MAIN MENU
Overview Basic Network Port System Monitor sAve [Restart] Exit
Restart the whole system or selected serial ports
Enter: select ESC: previous menu

10. Press **S** or use the arrow keys to select **System** and then press **ENTER** to restart the CN2600.

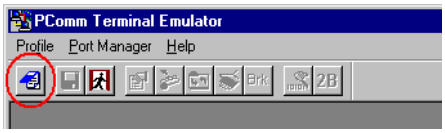


Serial Console

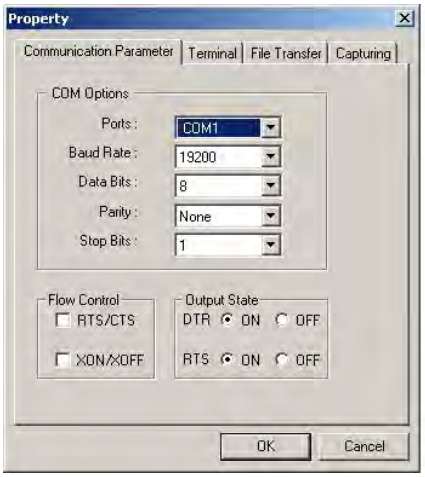
The CN2600 supports configuration through the serial console, which is the same as the Telnet console but accessed through the RS-232 console port rather than through the network. Once you have entered the serial console, the configuration options and instructions are the same as if you were using the Telnet console.

The following instructions and screenshots show how to enter the serial console using PComm Terminal Emulator, which is available free of charge as part of the PComm Lite suite. You may use a different terminal emulator utility, although your actual screens and procedures may vary slightly from the following instructions.

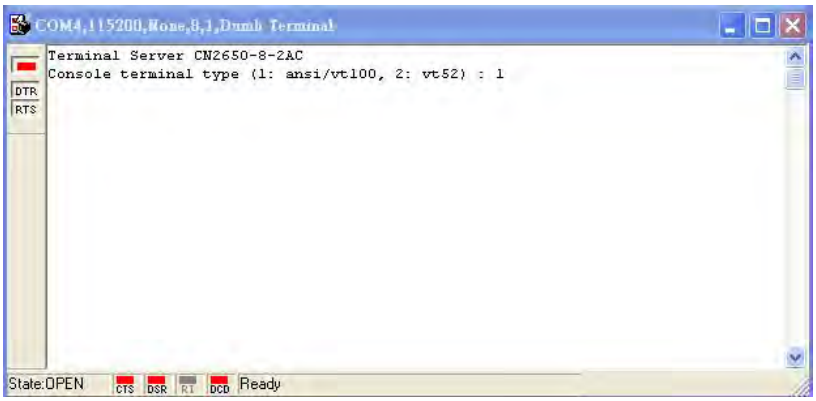
1. Use a serial cable to connect the CN2600's serial console port to your computer's male RS-232 serial port.
2. From the Windows desktop select **Start → All Programs → PComm Lite → Terminal Emulator**.
3. The PComm Terminal Emulator window should appear. From the **Port Manager** menu, select **Open**, or simply click the **Open icon** as shown below:



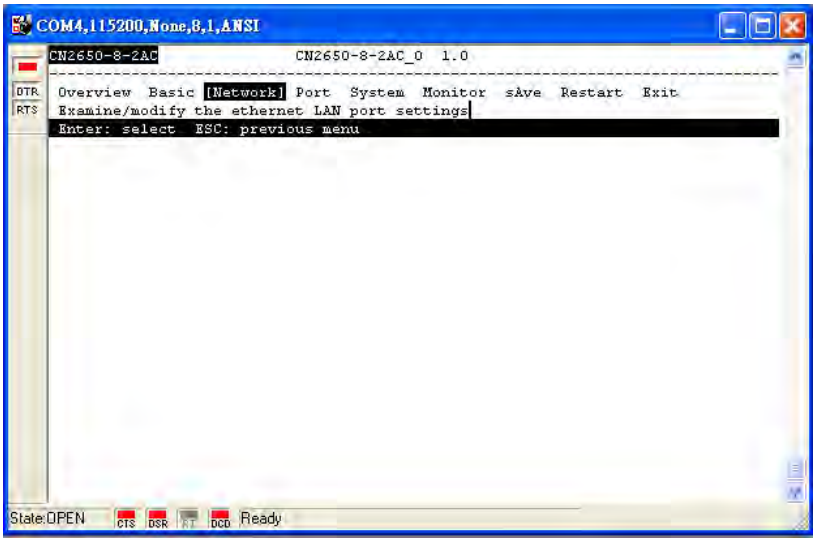
4. The Property window opens automatically. Select the **Communication Parameter** tab, and then select the appropriate COM port for the connection (COM1 in this example). Configure the baudrate for either 460800, 230400, 115200, 57600, 38400, 19200, or 9600, and then press **OK**.



5. From the Property window's Terminal page, select **ANSI** or **VT100** for **Terminal Type** and click **OK**.
6. Press <Enter> key to bring out the console screen. If the CN2600 has been set up for password protection, you will be prompted to enter the password. After you enter the password, or if password protection was not enabled, you will be prompted to select the terminal mode. Press **1** for **ansi/vt100** and then press **ENTER**.



7. The main menu should come up. Once you are in the console, you may configure the IP address through the **Network** menu item, just as with the Telnet console. Please refer to steps 4 to 11 in the *Telnet Console* section to complete the initial IP configuration.



4

Serial Port Operation Modes

In this chapter, we describe the various operation modes of the CN2600. CN2600 modes are grouped by type of application, such as Device Control or Reverse Terminal. The options include an operation mode that relies on a driver installed on the host computer, and operation modes that rely on TCP/IP socket programming concepts. After selecting the proper operation mode, please refer to Chapter 5, Configuration with the Web Console, for detailed information on configuration parameters.

The following topics are covered in this chapter:

- **Overview**
- **Device Control Applications**
  - Real COM Mode
  - RFC2217 Mode
- **Socket Applications**
  - TCP Server Mode
  - TCP Client Mode
  - UDP Mode
- **Redundant COM**
- **Dual-host Redundant Data Acquisition System (DRDAS)**
- **Terminal Applications**
  - Terminal ASCII Mode
  - Terminal BIN Mode
- **Reverse Terminal Applications**
  - Reverse Telnet
- **Dial In/Out Modes**
- **Disabled Mode**

Overview

The CN2600 network-enables traditional serial (RS-232/422/485) devices. The serial device server is a special-purpose computer equipped with a CPU and TCP/IP protocols that can bi-directionally translate data between the serial and Ethernet formats. Your own computer will be able to access, manage, and configure remote facilities and equipment over the Internet from anywhere in the world.

Traditional SCADA and data collection systems rely on serial ports to collect data from various kinds of instruments. Since the CN2600 network-enables instruments equipped with an RS-232, RS-422, or RS-485 communication port, your SCADA and data collection system will be able to access all instruments connected to a standard TCP/IP network, regardless of whether the devices are used locally or at a remote site.

The CN2600 is an external IP-based network device that allows you to expand the number of serial ports for a host computer on demand. As long as your host computer supports the TCP/IP protocol, you will not be limited by the host computer's bus limitation (such as ISA or PCI), nor will you be limited by the absence of drivers for various operating systems.

In addition to providing socket access, the CN2600 also comes with a Real COM/TTY driver that transmits all serial signals intact. This enables you to preserve your existing COM/TTY-based software without needing to invest in additional software.

Three different socket modes are available: TCP Server, TCP Client, and UDP Server/Client. The main difference between the TCP and UDP protocols is that TCP guarantees delivery of data by requiring the recipient to send an acknowledgement to the sender. UDP does not require this type of verification, making it possible to offer faster delivery. UDP also allows unicast or multi-unicast of data to one IP or groups of IP addresses.

The CN2600 also supports console management applications, including Reverse Telnet modes. Reverse terminal modes enable you to connect to a server's console port through an IP network for remote control and/or monitoring of that server.

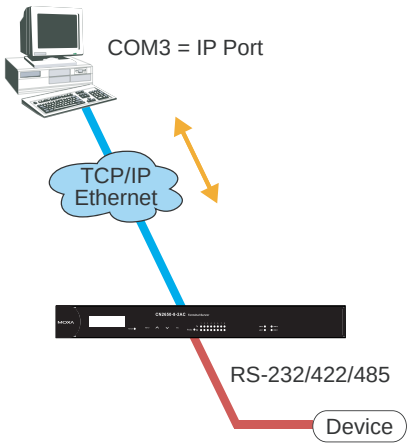
Device Control Applications

For device control applications, the CN2600 offers the following modes: Real COM and RFC2217 mode.

Real COM Mode

The CN2600 comes bundled with Real COM drivers for Windows 98/ME/NT/ 2000/XP/2003/Vista systems and TTY drivers for Linux systems.

In Real COM mode, the bundled drivers are able to establish a transparent connection between a host and a serial device by mapping the serial port on the CN2600 to a local COM/TTY port on the host computer. Real COM mode supports up to 8 simultaneous connections that enable multiple hosts to simultaneously collect data from the same serial device.



One of the major conveniences of using Real COM mode is that it allows you to use software that was written for pure serial communication applications. The Real COM driver intercepts data sent to the host's COM port, packs it into a TCP/IP packet, then redirects it through the host's Ethernet card. At the other end of the connection, the CN2600 accepts the Ethernet frame, unpacks the TCP/IP packet, and then transparently sends the data through the serial port to the attached serial device.

ATTENTION

Real COM mode allows several hosts to have access control over the same CN2600. The drivers that come with your CN2600 control host access by checking the host's IP address. Please refer to the *Accessible IP List* section in Chapter 8, *System Management Settings*, for more *details*.

RFC2217 Mode

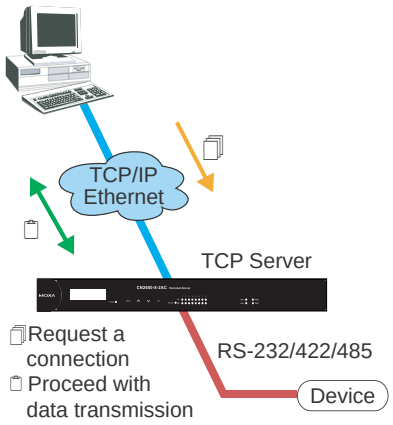
RFC-2217 mode is similar to Real COM mode. That is, a driver is used to establish a transparent connection between a host computer and a serial device by mapping the serial port on the CN2600 to a local COM port on the host computer. RFC2217 defines general COM port control options based on the Telnet protocol. Third party drivers supporting RFC-2217 are widely available on the Internet and can be used to implement Virtual COM mapping to your CN2600 serial port(s).

Socket Applications

For socket applications, the CN2600 offers the following modes: TCP Server, TCP Client and UDP.

TCP Server Mode

In TCP Server mode, the serial port on the CN2600 is assigned a port number which must not conflict with any other serial port on the CN2600. The host computer initiates contact with the CN2600, establishes the connection, and receives data from the serial device. This operation mode also supports up to 8 simultaneous connections, enabling multiple hosts to collect data from the same serial device at the same time.



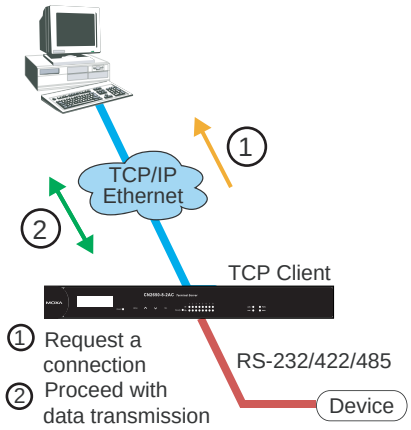
As illustrated in the figure, data transmission proceeds as follows:

The host requests a connection from the CN2600, which is configured for TCP Server mode.

Once the connection is established, data can be transmitted in both directions between the host and the CN2600.

TCP Client Mode

In TCP Client mode, the CN2600 can actively establish a TCP connection to a pre-defined host computer when serial data arrives.



After the data has been transferred, the CN2600 can automatically disconnect from the host computer by using the **Inactivity time** settings.

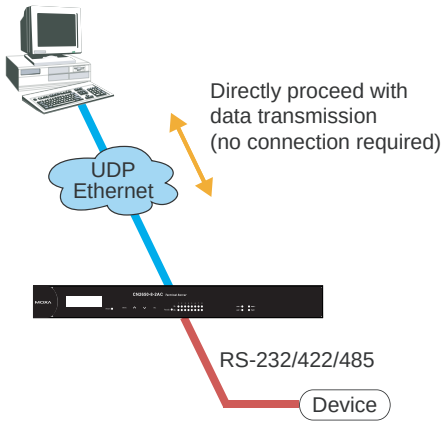
As illustrated in the figure, data transmission proceeds as follows:

The CN2600, configured for TCP Client mode, requests a connection from the host.

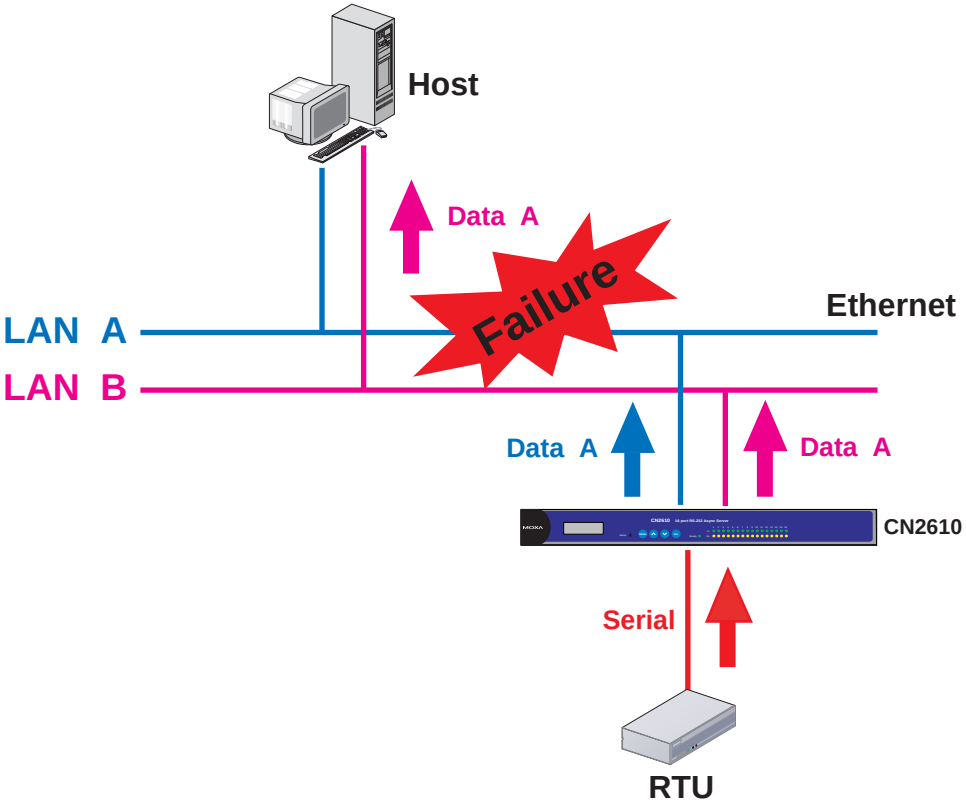
Once the connection is established, data can be transmitted in both directions between the host and the CN2600.

UDP Mode

Compared to TCP communication, UDP is faster and more efficient. In UDP mode, you can unicast or multi-unicast data from a serial device to one or multiple host computers and the serial device can receive data from one or multiple host computers. These traits make UDP mode especially suited for message display applications.



Redundant COM

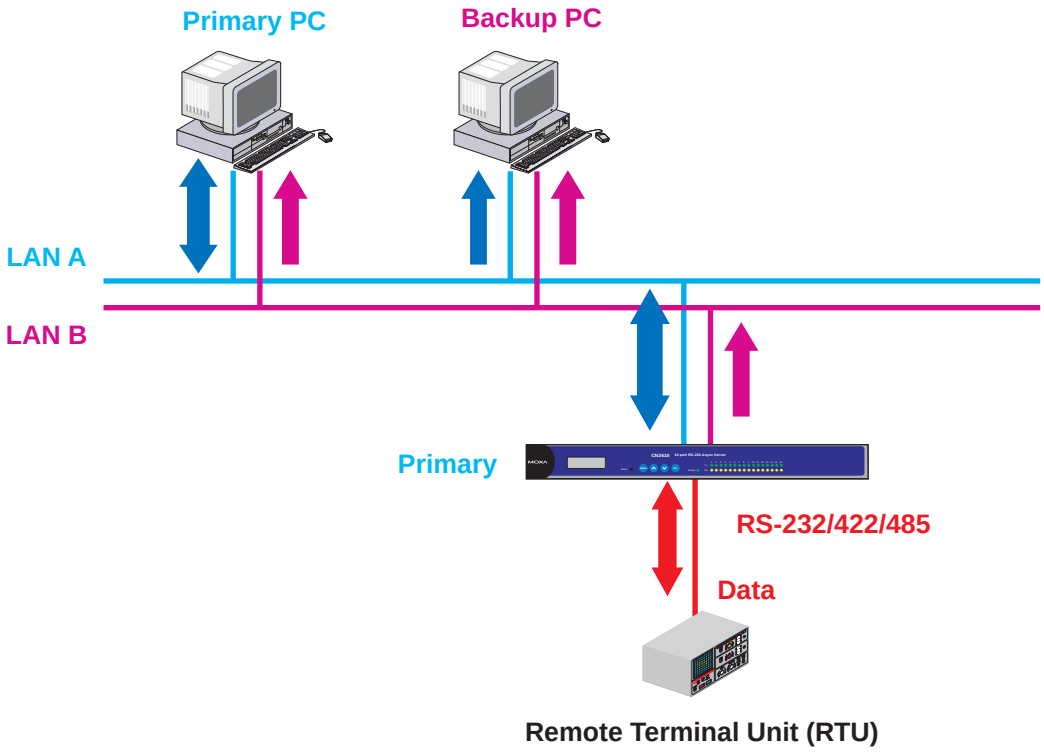


The Redundant COM operation mode can be used to set up a redundant LAN between the serial devices connected to the CN2600's serial ports and the host computer. The redundant structure involves using the CN2600's two LAN ports to set up two independent LANs that connect the CN2600 to the host computer. If either of the two LANs fails, the other LAN will continue transmitting packets between the serial devices and the host, with the packets passing through the CN2600. In fact, one of the biggest advantages of the CN2600's Redundant COM mode is that the "switching time" is zero.

ATTENTION

1. If either LAN gets disconnected, it will take at least 1 minute for the LAN to recover after reconnecting.
2. If both LANs get disconnected, you will need to re-open your application software's COM port for data to transmit properly.

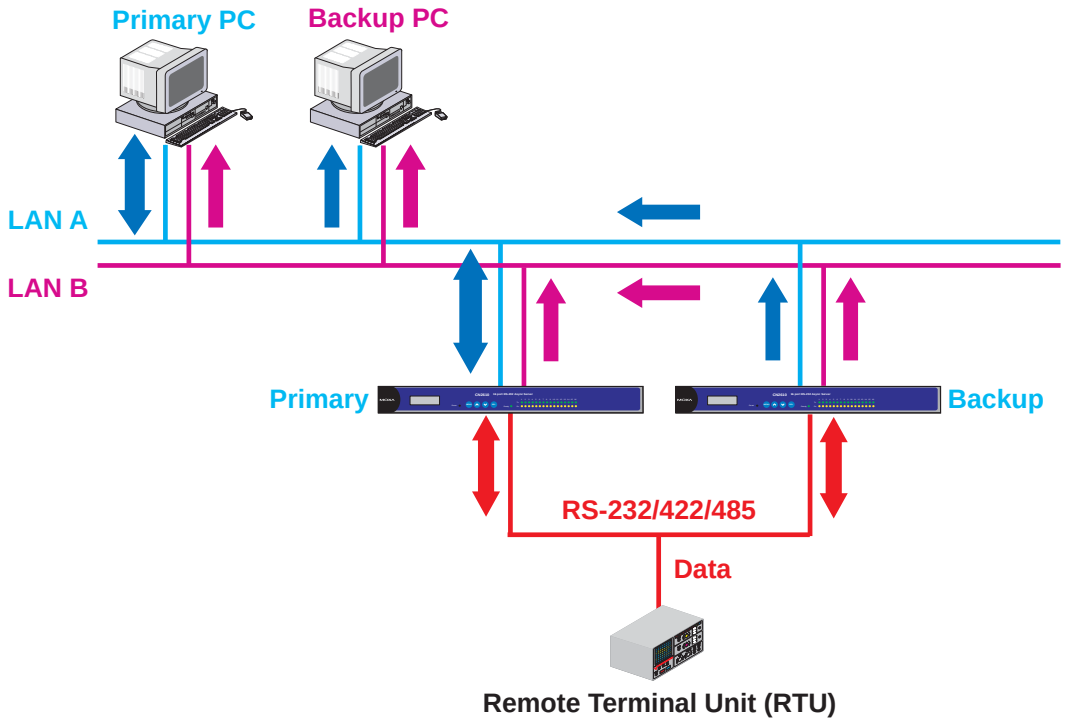
Dual-host Redundant Data Acquisition System (DRDAS)



The DRDAS operation mode provides a highly redundant network structure that takes advantage of the CN2600's dual LAN ports, dual IP addresses, and dual MAC addresses. DRDAS uses a backup PC that is set up to take over when the primary PC fails.

The CN2600's dual-host redundant configuration sends serial data to 4 IP addresses on the network. Users select a Primary IP and 3 Secondary IPs. When the Primary IP fails, the backup IPs take over by using the switching library (refer to Chapter 12 for more details).

With this kind of redundant setup, if one of the secondary IPs tries to send commands to the serial device, the commands are discarded by the CN2600, since only the Primary IP is allowed to conduct bi-directional transmission. The backup IPs are only allowed to receive data from the CN2600.

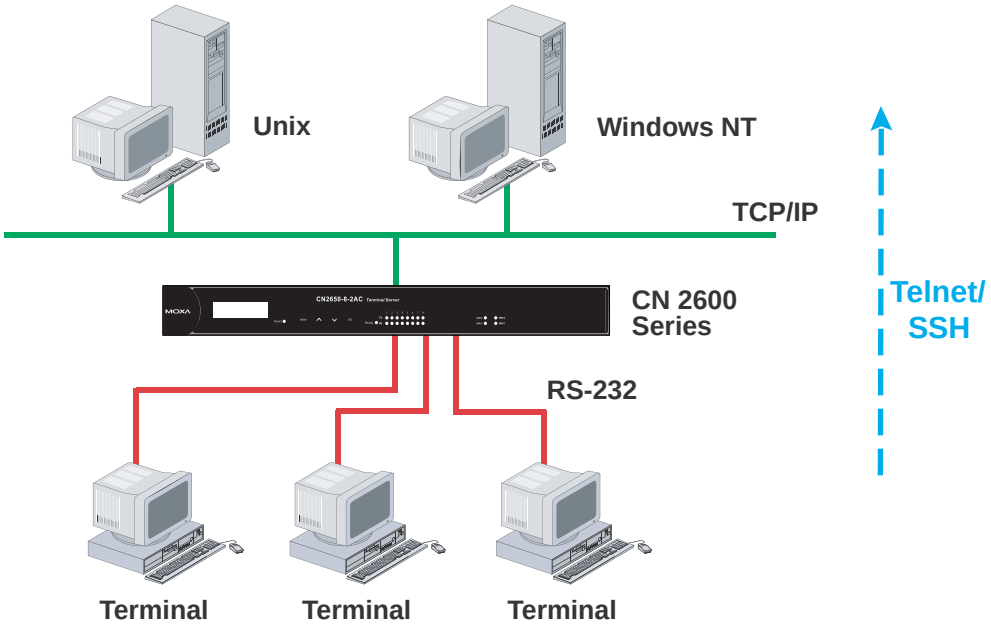


This type of highly redundant setup is implemented with two CN2600 terminal servers, as shown above in the structure diagram. All aspects of the system are backed up, including the PC hosts, the networks, and the CN2600 terminal servers. The entire system will continue operating in the following situations:

1. When the Primary PC and LAN A fail at the same time (the backup PC and LAN B will take over).
2. When the Primary PC and the Primary CN2600 fail at the same time (the backup PC and the backup CN2600 will take over).
3. When LAN A and the Primary CN2600 fail at the same time (LAN B and the backup CN2600 will take over).

NOTE The RS-232 connector on the Remote Terminal Unit (RTU) shown above must be set up with an RS-232 to RS-422/485 converter, such as the Moxa TCC-100I, to convert RS-232 signals to RS-485 signals. The connectors on the two CN2600 terminal servers will also need to use converters, such as the Moxa TCC-100I. In this way, users can take advantage of RS-485's multi-drop feature to share data with the secondary CN2600.

Terminal Applications



Terminal applications involve connecting terminals to UNIX or Windows servers over a network. A terminal connects to the appropriately configured serial port the CN2600, and the CN2600 transmits information to and from a UNIX or Windows server over the network through its Ethernet port. You may need to check with your network administrator to determine the appropriate terminal mode. All terminal modes support fast keys as used in many terminal applications.

Please refer to Chapter 4, Introducing Serial Port Operation Modes, for detailed information and configuration instructions.

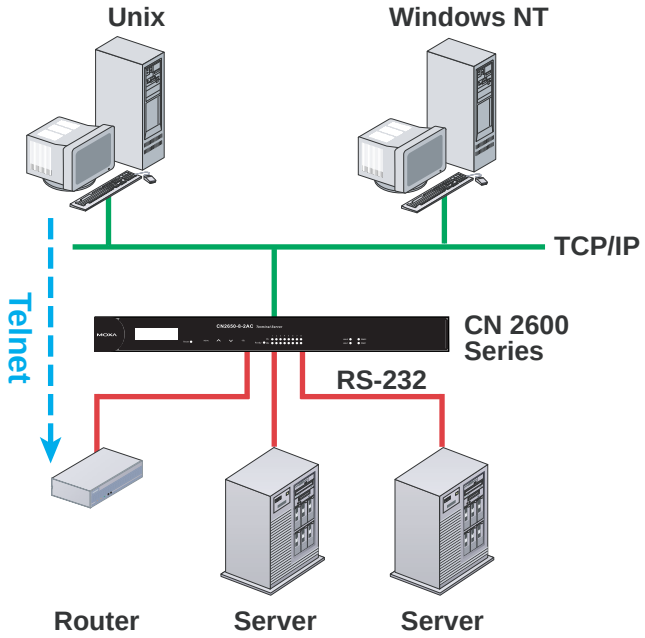
Terminal ASCII Mode

Terminal ASCII mode can handle up to 8 sessions per port with the ability to switch between sessions on the same terminal. This mode is used for text-based terminals with no file transfer capability or encryption.

Terminal BIN Mode

Terminal BIN mode allows one session per port and is used for terminal applications that include file transfer features.

Reverse Terminal Applications



Reverse terminal applications are similar to terminal applications in that they involve using the CN2600 to manage the connection between a terminal and a server. The difference is that with reverse terminal applications, the terminal is connected through the network and the server is connected through the serial port, rather than the other way around. In practice, a reverse terminal session typically involves a network administrator telnetting to a device that has a dedicated serial console port used specifically for configuration purposes.

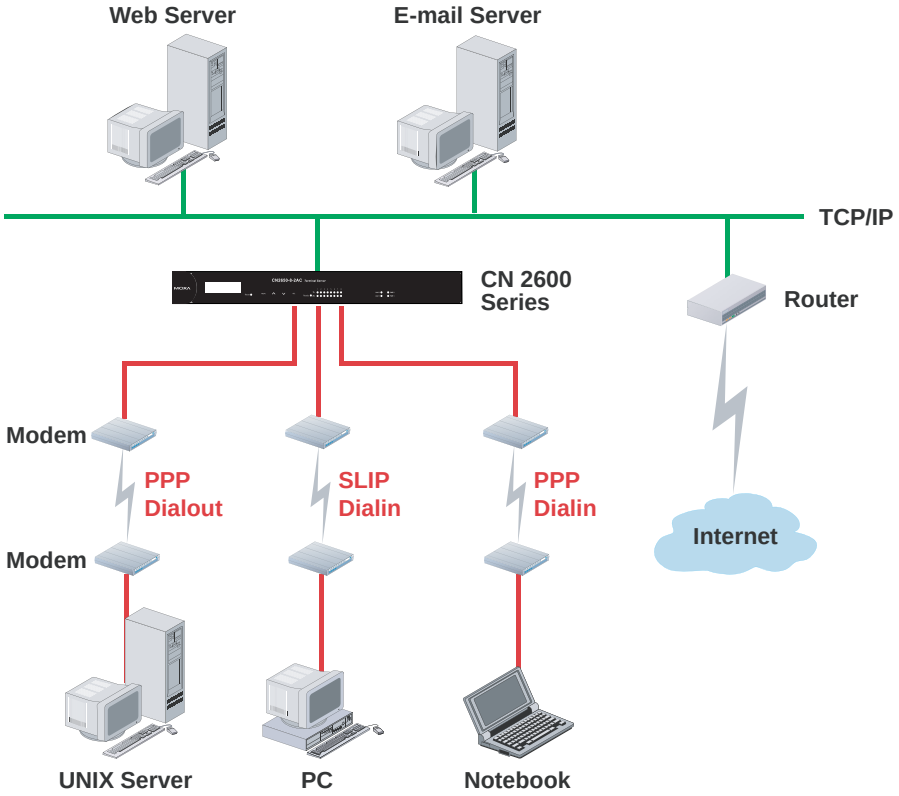
For example, many routers, switches, UPS units, and other devices (including the CN2600) have Console/AUX or COM ports to which a terminal can be physically connected for console management. With the CN2600, the device's console port can be connected to a serial port on the CN2600, allowing a network administrator to telnet to the device remotely through the network. Although modern network equipment generally allows other options for remote configuration through the network, there are situations in which it is necessary or desirable to configure a device by serial console (e.g., for security reasons, when using older-generation equipment, or as a backup configuration method when the network is down).

CN2600 reverse terminal modes allow the use of the CN2600 User Table or a RADIUS server for identity verification purposes. Please refer to the Misc. Network Settings section in Chapter 8, System Management Settings, for instructions on setting up the CN2600 User Table.

Reverse Telnet

Reverse Telnet mode is widely used for device management in telecommunication control rooms. The system waits for a host on the network to initiate a connection. Since TCP Server mode does not assist with conversion of CR/LF commands, reverse terminal applications that require this conversion should use Reverse Telnet mode.

Dial In/Out Modes



The CN2600 provides dial-in/dial-out access for ISPs and enterprises that need a remote access solution. When a user at a remote site uses a PPP dial-up connection to access the CN2600, the CN2600 plays the role of a dial-up server, but also ensures that the user has legal access to the network by verifying the user's identity with the CN2600 User Table or a RADIUS server. Please refer to the Misc. Network Settings section in Chapter 8, System Management Settings, for instructions on setting up the CN2600 User Table.

The CN2600 supports PPP, SLIP, and Terminal modes for dial-in/dial-out access. Regardless of which operating system is used, you will always be able to use standard PPP dial-up to establish a connection. The CN2600 can also act as a router to connect serial ports to a WAN connection. Routing protocols (including static, RIP I, and RIP II) can be adjusted to route different WAN connections.

Please refer to Chapter 5, Configuration with Web Console, for detailed information and configuration instructions.

Disabled Mode

You can disable any port on the CN2600 by setting the operation mode to **Disabled**.

5

Configuration with the Web Console

The web console is the most user-friendly method available to configure the CN2600. With a standard web browser, you have easy and intuitive access to all settings and options. In this chapter, we introduce the web console and go through the basic configuration options. The same configuration options are also available through the Telnet and serial console.

This chapter covers the following topics:

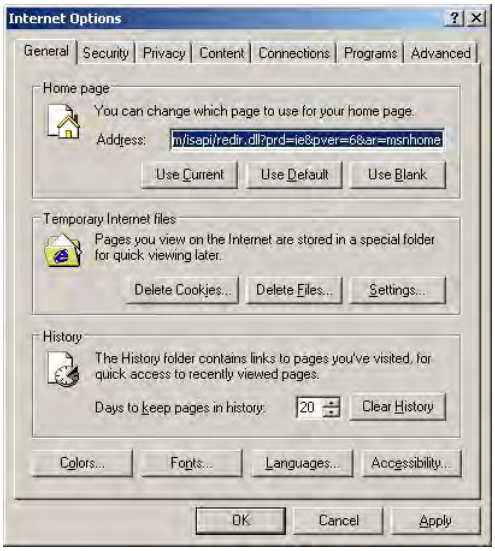
- **Using Your Web Browser**
  - Browser Cookie Settings
  - Trusted Site Settings
  - Opening the Web Console
- **Web Console Navigation**
- **Basic Settings**
  - Server Settings
  - Time Settings
- **Network Settings**
  - Basic Network Settings
  - Advanced Network Settings
  - Configuring the Route Table

Using Your Web Browser

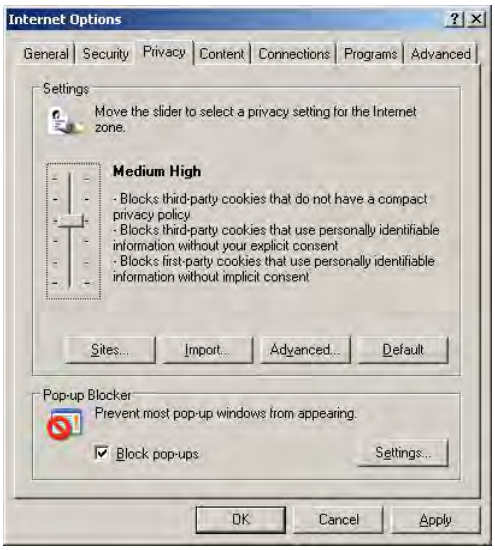
Browser Cookie Settings

Verify that cookies are enabled for your browser. If the cookies are disabled, you will not be able to use the web console. (Cookies are only used for password transmission.)

1. For Internet Explorer, enable cookies by selecting Internet Options from the Tools menu:



2. Select the **Privacy** tab. There are six levels of privacy setting: Block All Cookies, High, Medium High, Medium, Low, and Accept All Cookies. Users must select **Medium High** (as the image shows) or below to access the CN2600 web console.



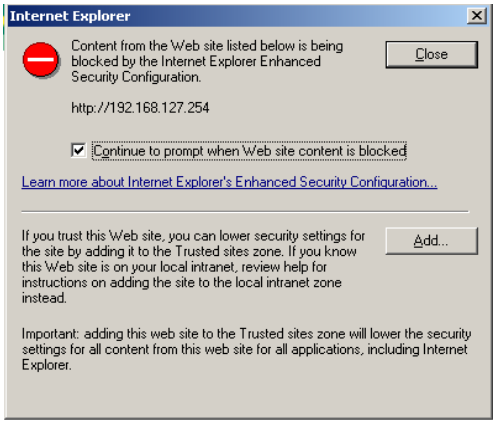
ATTENTION

If you are not using Internet Explorer, cookies are usually enabled through a web browser setting such as "allow cookies that are stored on your computer" or "allow per-session cookies."

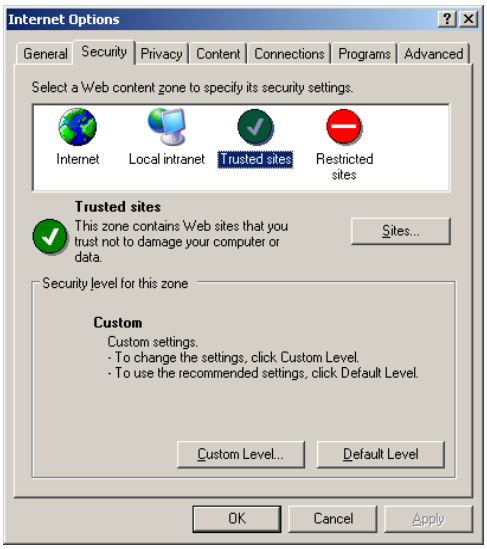
Trusted Site Settings

For Windows 2003 users, you may need to add the CN2600's IP address to your browser's list of trusted sites.

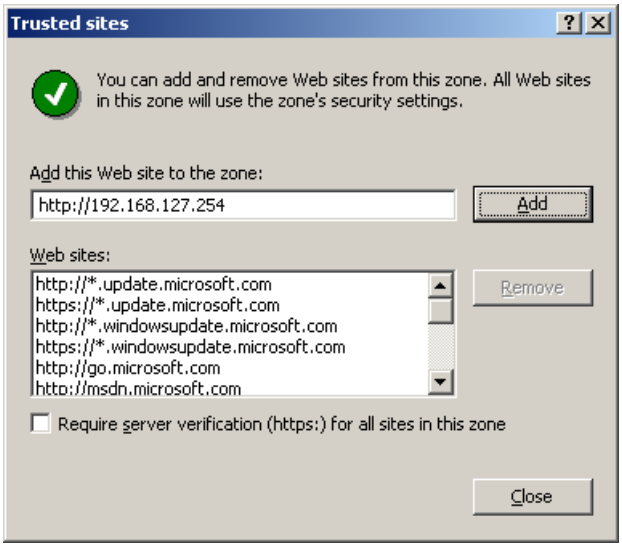
1. If you see the following window while attempting to view the web console, click on Add… to modify the list of trusted sites:


Internet Explorer
Content from the Web site listed below is being blocked by the Internet Explorer Enhanced Security Configuration.
Close
http://192.168.127.254
Continue to prompt when Web site content is blocked
Learn more about Internet Explorer's Enhanced Security Configuration...
If you trust this Web site, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this Web site is on your local intranet, review help for instructions on adding the site to the local intranet zone instead.
Add...
Important: adding this web site to the Trusted sites zone will lower the security settings for all content from this web site for all applications, including Internet Explorer.

You may also directly access the list of trusted sites through **Internet Options** in the **Tools** menu of Internet Explorer. Select the **Security** tab, then click on the **Trusted Sites icon** and on the **Sites…** button:



2. In either case, the window below should appear, showing the list of sites that you have configured Internet Explorer to trust. Add the IP address of your CN2600 here (the factory default LAN1 IP address is 192.168.127.254 and default LAN2 IP address is 192.168.126.254.)



After adding the CN2600's IP address as a trusted site, you should be able to view the web console by entering the CN2600's IP address in your browser's address bar.

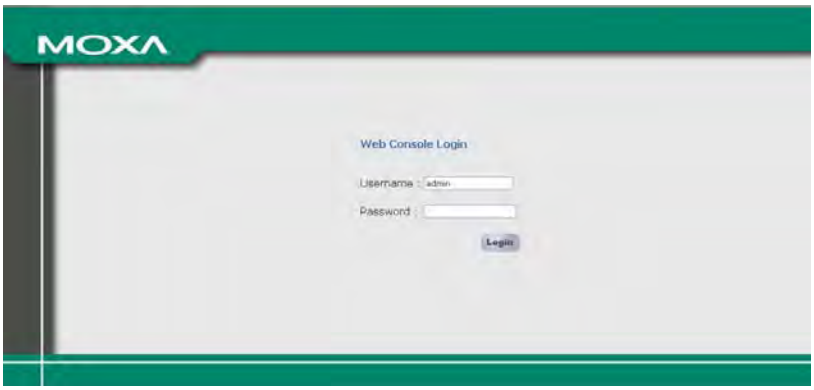
Opening the Web Console

Open your web browser and enter **192.168.127.254** in the website address line. This is the default IP address for the CN2600–if a new address has been assigned, enter the new address instead. Press **ENTER** to load the page.

ATTENTION

The examples and figures in this chapter use the CN2600 factory default IP address of 192.168.127.254. If you have assigned a different IP address to your CN2600, be sure to adjust accordingly when following these directions. Please refer to **Chapter 3**, ***Initial IP Address Configuration***, for details on how to configure the IP address.

3. Enter the console password if prompted. (This will not apply if you did not enable password protection for your CN2600.) The password will be transmitted with MD5 encryption over the Ethernet.



ATTENTION

If you forget your password, the ONLY way to configure the CN2600 is by using the reset button to reset all settings and load the factory defaults. If you have disabled the reset button in your CN2600 configuration, you may still use it to load the factory defaults within the first 60 seconds that the CN2600 is powered on.

Remember to back up your configuration by exporting it to a file. Your configuration can be easily restored by importing the file to the CN2600. This will save time if you have forgotten the password and need to reload the factory defaults.

4. The CN2600's web console will appear.

Web Console Navigation

In the CN2600 web console, the left panel is the navigation panel and contains an expandable menu tree for navigating among the various settings and categories. When you click on a menu item in the navigation panel, the main window will display the corresponding options for that item. Configuration changes can then be made in the main window. For example, if you click on **Basic Settings** in the navigation panel, the main window will show a page of basic settings that you can configure.

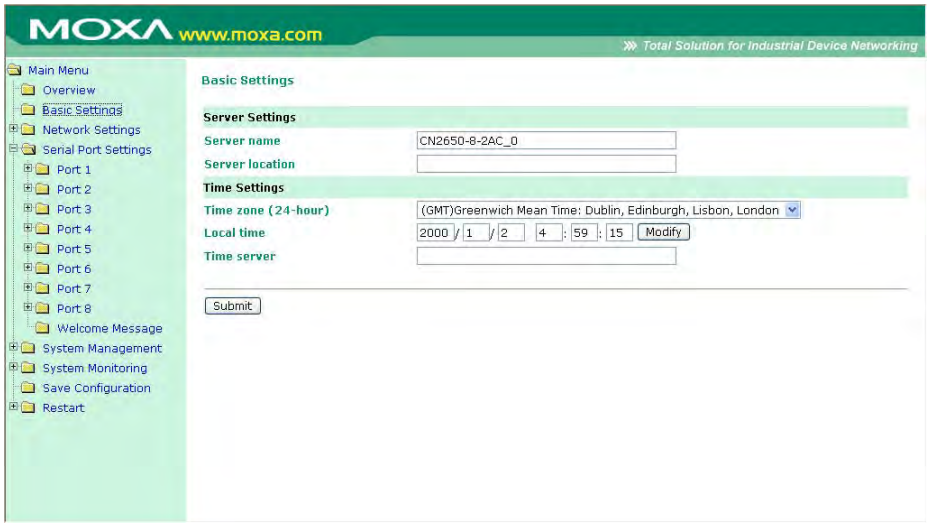
You must click on the **Submit** button to keep your configuration changes. The **Submit** button will be located at the bottom of every page that has configurable settings. If you navigate to another page without clicking the Submit button, your settings will not be retained.

Changes will not take effect until they are saved and the NPort is restarted! You may complete this in one step by clicking on the **Save/Restart** option after you submit a change. If you need to make several changes before restarting, you may save your changes without restarting by selecting **Save Configuration** in the navigation panel. If you restart the CN2600 without saving your configuration, the CN2600 will discard all submitted changes.

Basic Settings

You may access Basic Settings in the navigation panel.

Server Settings



Server name: This is an optional free text field for your own use; it does not affect operation of the CN2600. It can be used to help differentiate one CN2600 server from another.

Server location: This is an optional free text field for your own use; it does not affect operation of the CN2600. It is useful for assigning or describing the location of a CN2600. In a network environment of multiple servers, this can be a valuable aid when performing maintenance.

Time Settings

The CN2600 has a built-in Real-Time Clock for time calibration functions. Functions such as Auto Warning Email or SNMP Trap can add real-time information to messages.

Before making any adjustments to the time, first select the correct time zone and submit the change. The console will display the real time according to the time zone. To modify the real time clock, click on **Modify** next to the **Local time** field. Once you submit the new time, the CN2600's firmware will modify the GMT time according to your time zone and local time settings.

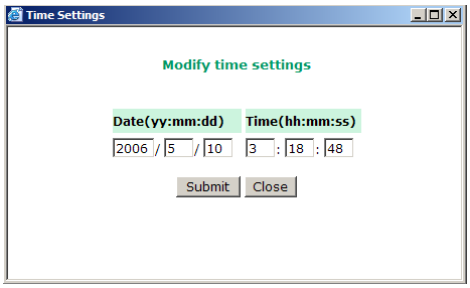
ATTENTION

There is a risk of explosion if the real-time clock battery is replaced with the wrong type!

The CN2600's real time clock is powered by a lithium battery. We strongly recommend that you do not attempt replacement of the lithium battery without help from a qualified Moxa support engineer. If you need to change the battery, please contact the Moxa RMA service team.

Time zone (default=GMT Greenwich Mean Time): This field shows the currently selected time zone and allows you to select a different time zone.

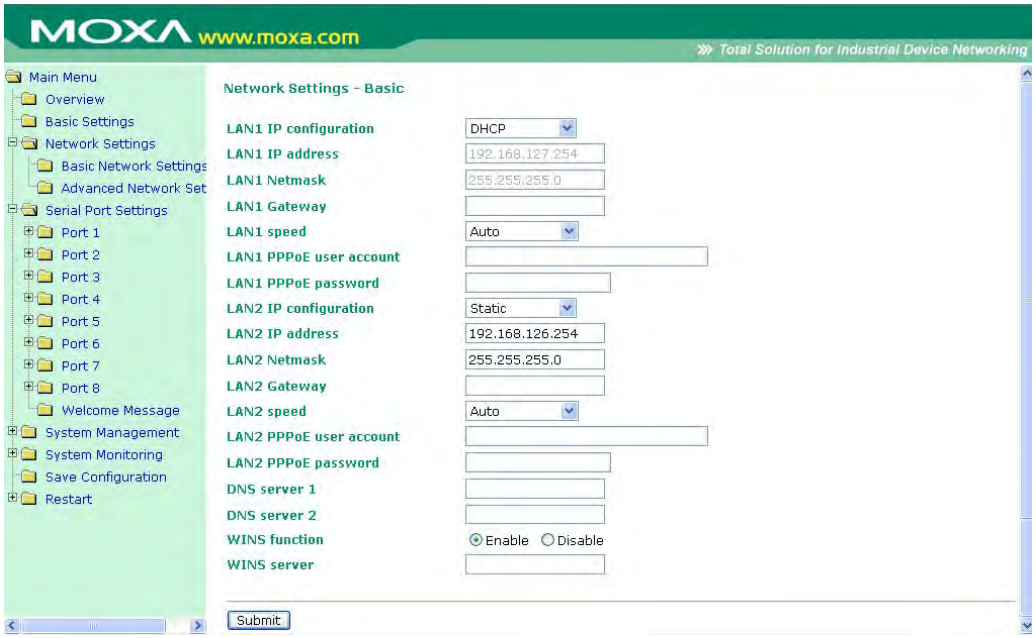
Local time: This field shows the time that you last opened or refreshed the browser. To set the local time for the CN2600, click on the **Modify…** button, then submit your changes in the screen as shown below.



Time server: The CN2600 uses SNTP (RFC-1769) for auto time calibration. You may enter a time server IP address or domain name in this optional field. Once the CN2600 is configured with the correct time server address, it will request time information from the time server every 10 minutes.

Network Settings

Basic Network Settings



You can access **Basic Network Settings** by expanding the **Network Settings** item in the navigation panel. Basic Network Settings is where you assign the CN2600's IP address, netmask, Gateway, and other IP parameters.

NOTE: You must assign a valid IP address to your CN2600 before it will work in your network environment. Your network system administrator should provide you with a unique IP address and related settings for your network. First-time users can refer to ***Chapter 3: Initial IP Address Configuration***, for more information.

IP configuration (default=Static): You can choose from four possible IP configuration modes.

Option	Description
Static	User-defined IP address, netmask, gateway.
DHCP	DHCP server-assigned IP address, netmask, gateway, DNS, and time server
DHCP/BOOTP	DHCP server-assigned IP address, netmask, gateway, DNS, and time server, or BOOTP server-assigned IP address (if the DHCP server does not respond)
BOOTP	BOOTP server-assigned IP address
PPPoE	PPP over Ethernet, remote ISP-assigned IP address

IP Address (LAN1 default = 192.168.127.254; LAN2 default = 192.168.126.254): Enter the IP address that will be assigned to your CN2600. All ports on the CN2600 will share this IP address. An IP address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IP address to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your network environment.

Netmask (default=255.255.255.0): Enter the subnet mask. A subnet mask represents all of the network hosts at one geographic location, in one building, or on the same local area network. When a packet is sent out over the network, the CN2600 will use the subnet mask to check whether the desired TCP/IP host specified in the packet is on the local network segment. If the address is on the same network segment as the CN2600, a connection is established directly from the CN2600. Otherwise, the connection is established through the given default gateway

Gateway: Enter the IP address of the gateway if applicable. A gateway is a network computer that acts as an entrance to another network. Usually, the computers that control traffic within the network or at the local Internet service provider are gateway nodes. The CN2600 needs to know the IP address of the default gateway computer in order to communicate with the hosts outside the local network environment. For correct gateway IP address information, consult the network administrator.

ATTENTION

In dynamic IP environments, the firmware will try to get the network settings from the DHCP or BOOTP server 3 times every 30 seconds until network settings are assigned by the DHCP or BOOTP server. The first try times out after 1 second, the second after 3 seconds, and the third after 5 seconds.

If the DHCP/BOOTP server is unavailable, the firmware will use the default IP address (192.168.127.254), netmask, and gateway settings.

DNS server 1: This is an optional field. If your network has access to a DNS server, you may enter the DNS server's IP address in this field. This allows the CN2600 to use domain names instead of IP addresses to access hosts.

Domain Name System (DNS) is the way that Internet domain names are identified and translated into IP addresses. A domain name is an alphanumeric name, such as www.moxa.com, that it is usually easier to remember than the numeric IP address. A DNS server is a host that translates this kind of text-based domain name into the actual IP address used to establish a TCP/IP connection. When the user wants to visit a particular website, the user's computer sends the domain name (e.g., www.moxa.com) to a DNS server to request that website's numeric IP address. When the IP address is received from the DNS server, the user's computer uses that information to connect to the website's web server.

The CN2600 will play the role of a DNS client, in the sense that it will actively query the DNS server for the IP address associated with a particular domain name. The following functions on the CN2600 web console support the use of domain names in place of IP addresses: Time Server, Destination IP Address (in TCP Client mode), Mail Server, SNMP Trap Server, Destination Address (in Pair Connection mode), Primary/Secondary Host Address (in Terminal mode), RADIUS Server and SMTP Server.

DNS server 2: This is an optional field. The IP address of another DNS server may be entered in this field for times when DNS server 1 is unavailable.

PPPoE user account and **PPPoE password**: For dynamic broadband networks such as xDSL or cable modem, users must enter the username and password that they received from their ISP to establish network connection. If a serial port on the CN2600 will be using PPPoE, enter the account name and password in these fields.

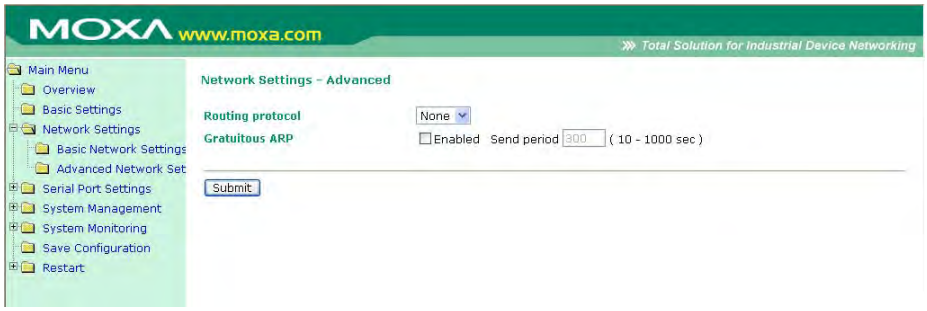
WINS function (default=enable): Enable or disable the WINS (Windows Internet Naming Service) server.

WINS server: If a WINS Server is connected to the network, enter the WINS Server's IP address in this field. TCP/IP uses IP addresses to identify hosts, but users often use symbolic names, such as computer names. The WINS Server, which uses NetBIOS over TCP/IP, contains a dynamic database to map computer names to IP addresses.

LAN speed (default=Auto): You may configure the network speed for the built-in Ethernet connection on the CN2600. IEEE802.3 Ethernet supports auto negotiation of transfer speed. However, some switches/hubs require that the communication speed be fixed at 100Mbps or 10Mbps.

Advanced Network Settings

You can access **Advanced Network Settings** by expanding the Network Settings item in the navigation panel. Advanced Network Settings is where the routing protocol and gratuitous ARP are configured.



What is RIP?

RIP (Routing Information Protocol) is a protocol used to manage routing information within a self-contained network, such as a corporate LAN (Local Area Network) or an interconnected group of such LANs.

By using RIP, a gateway host with a router can send its entire routing table, which lists all the other hosts it knows about, to its closest neighbor host every 30 seconds. The neighbor host in turn will pass this information on to its closest neighbor, and so on, until all hosts within the network have the same routing path information. This state is known as network convergence. RIP uses a hop count as a way of determining network distance. (Other protocols use more sophisticated algorithms that also include timing.) After receiving a packet headed for a specific destination, a network host with a router uses the routing table information to determine the next host to route

the packet to.

RIP is considered an effective solution for small homogeneous networks. For larger, more complicated networks, transmitting the entire routing table every 30 seconds can bog down the network with a lot of extra traffic.

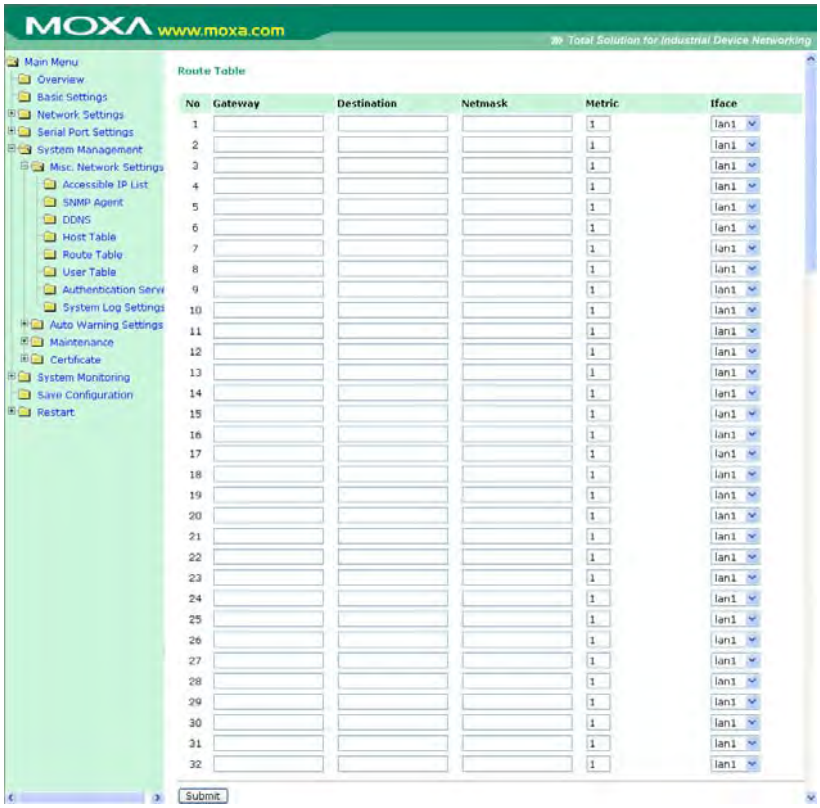
RIP 2 is an extension of RIP. Its purpose is to expand the amount of useful information contained in RIP packets, and to add security elements. RIP 2 has become the standard version of RIP, and the original RIP is no longer used.

Routing Protocol: You may select which routing protocol, if any, your network will employ.

Gratuitous ARP: In some applications, you may need the CN2600 to send broadcast packets to update the ARP table on the server. If you enable this function and set the send period, the CN2600 will send periodically send broadcast packets at the specified time interval.

Configuring the Route Table

You can access the **Route Table** by expanding **System Management** and then **Misc. Network Settings** in the navigation panel. The route table is where you configure how the CN2600 will connect to an outside network.



You are allowed up to 32 entries in the route table. For each entry, you must provide information on the gateway, destination, netmask, metric hops, and interface.

Gateway: This is the IP address of the next-hop router.

Destination: This is the host's IP address or the network address of the route's destination.

Netmask: This is the destination network's netmask.

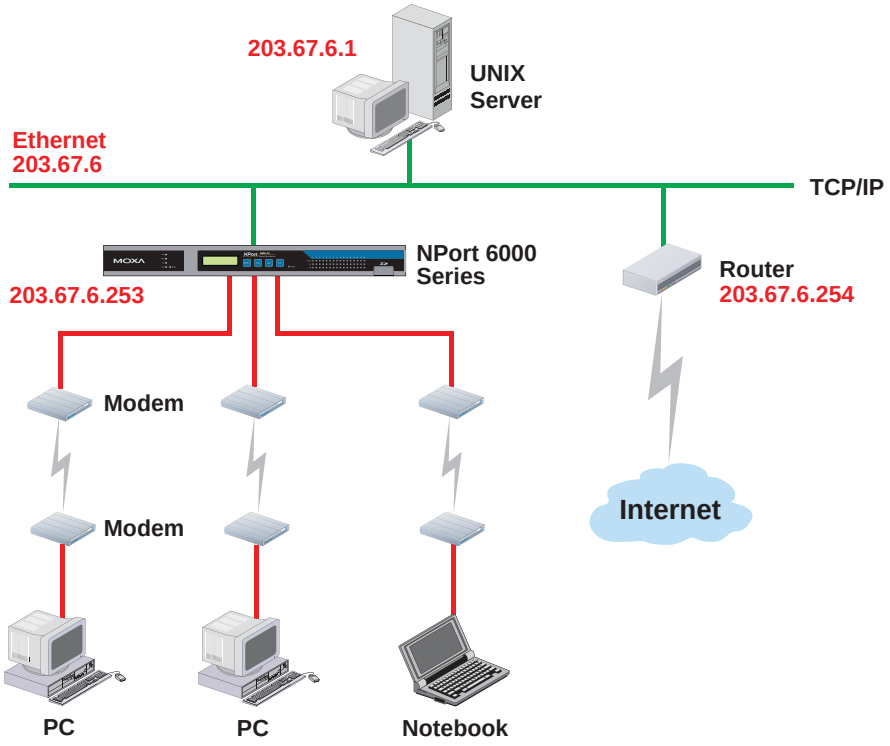
Metric: Enter the number of hops from the source to the destinationto allow the CN2600 to prioritize the routing of data packets if more than one router is available.

Iface: This is the network interface to which the packet must be sent.

ATTENTION

When a serial port is configured for PPP/SLIP, the **Iface** field must be set to that serial port for proper communication.

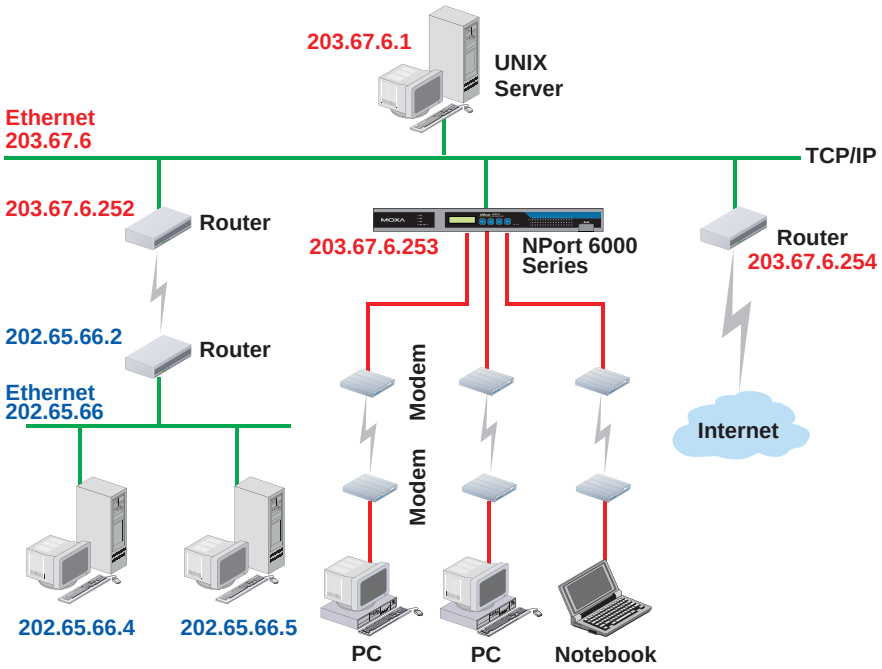
Configuring Routes to the Internet



In this example, the Notebook PC dials into the CN2600 to request a connection to the Internet host at **210.48.96.9**, which is not on the local network **203.67.6.***xxx*. This causes the CN2600 to act as a router and send the datagram to the default next-hop router, **203.67.6.254**. In this case, we should add the gateway IP address of **203.67.6.254** to the routing table to handle hops to **210.48.96.9**.

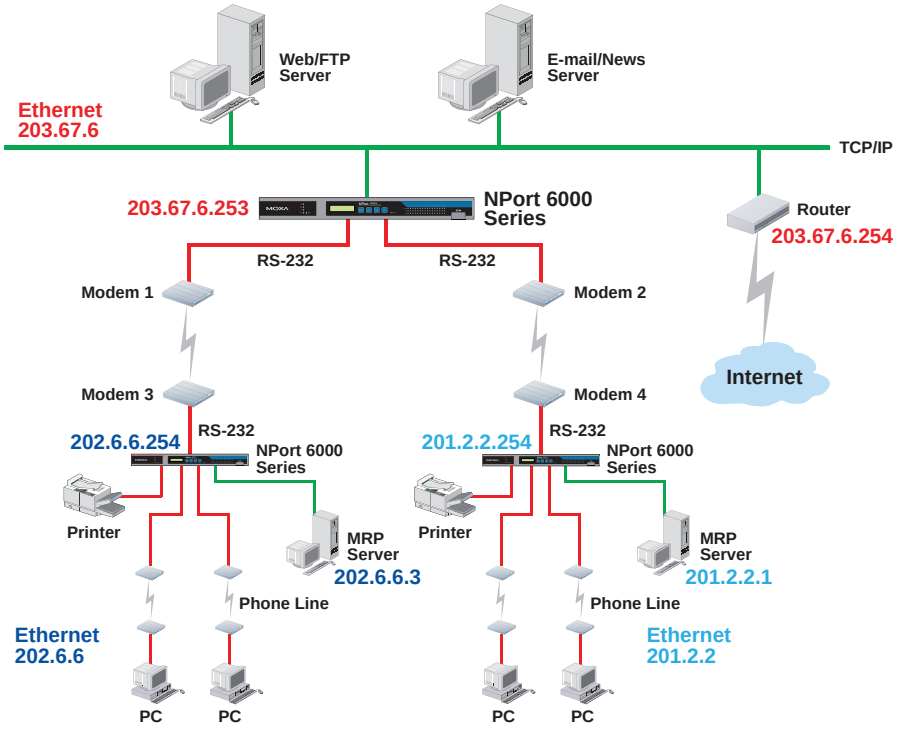
Generally, connections to the Internet are handled by assigning a gateway server in the network settings rather than through the route table.

Configuring Routes to the Intranet



In this example, dial-in users can make requests to Intranet hosts **202.65.66.4** or **202.65.66.5**, which are on network **202.65.66.***xxx* (located outside network **203.67.6**.*xxx*). You will need to add a route entry for the next-hop router, **203.67.6.252** that delivers requests to network **202.65.66.***xxx*. The metric hop in this case is 2 route hops.

Configuring Multiple-Point Routes

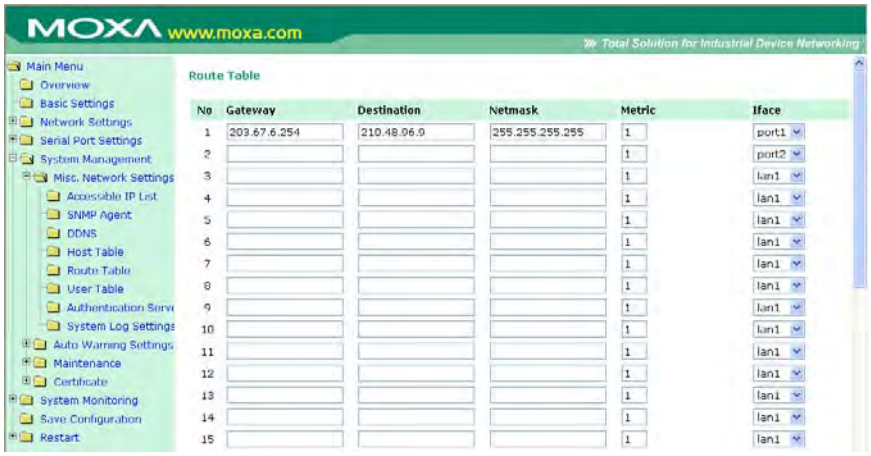


For multi-location enterprises, CN2600 servers can be placed in different branch offices and used as both multi-point routers and as remote access servers. When hosts (e.g., the Web/FTP and E-mail/News servers shown in the figure) send requests to hosts on another network, such as **202.6.6.***xxx* or **201.2.2.***xxx*, the corresponding CN2600 delivers the request to the another CN2600 on the remote end, **202.6.6.254** or **201.2.2.254**, as the next-hop router..

For this example, assume that Modem 1 is connected to serial port 1, Modem 2 is connected to serial port 2, and PPP source and destination IP addresses of modems 1, 2, 3, and 4 are as follows:

	Source IP	Destination IP		Source IP	Destination IP
Modem 1	203.67.6.250	202.6.6.250	Modem 3	202.6.6.250	203.67.6.250
Modem 2	203.67.6.249	201.2.2.249	Modem 4	201.2.2.249	203.67.6.249

In this case, you will need to add two entries to the routing table, as shown in the following figure.



6

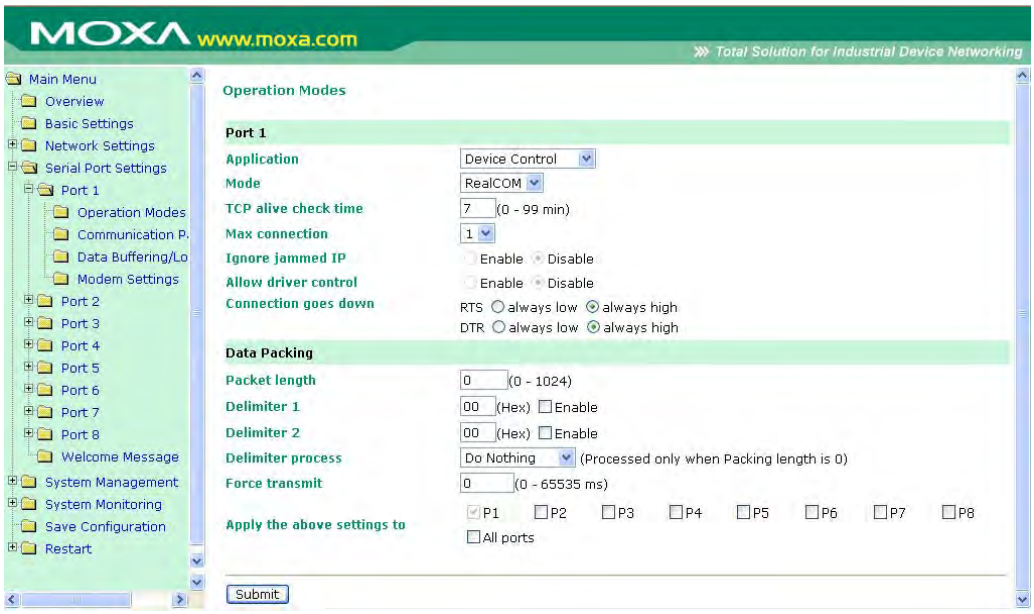
Configuring Serial Port Operation Modes

In this chapter, we explain how to configure the individual serial port modes. This chapter covers the following topics:

- **Port Setting Basics**
- **Device Control Applications**
  - Real COM Mode
  - RFC2217 Mode
- **Socket Applications**
  - TCP Server Mode
  - TCP Client Mode
  - UDP Mode
- **Redundant COM**
- **DRDAS**
  - DRDAS Real COM
  - DRDAS TCP Server
- **Terminal Applications**
  - Terminal ASCII (TERM_ASC)
  - Terminal BIN (TERM_BIN)
- **Reverse Terminal**
- **Dial In/Out Applications**
  - PPP Mode
  - PPPD Mode
  - SLIP Mode
  - SLIPD Mode
  - Dynamic Mode
- **Disabled Mode**

Port Setting Basics

Each serial port on the CN2600 can be configured independently. To configure the operation mode and settings for a port, expand **Serial Port Settings** in the navigation panel, then expand the port that you would like to configure. Individual port settings are grouped into four categories in the navigation panel: Operation Modes, Communication Parameters, Data Buffering/Log, and Modem Settings.



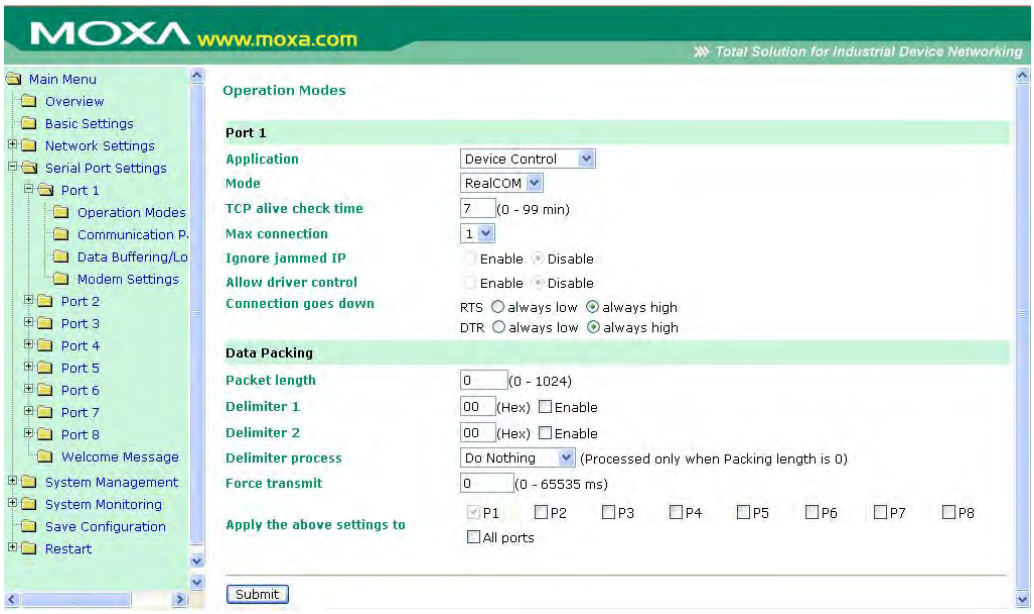
Select **Operation Modes** in the navigation panel to select and configure the mode for each serial port. For CN2600 models with 2 or more serial ports, you may use the checkboxes at the bottom of the window to apply the settings to one or more ports.

Application: Select an application for the serial port from among the choices. Your application will determine the modes that are available.

Mode: Once you have chosen an application, select the mode. The available configuration settings will vary depending on the mode that you have selected.

Device Control Applications

Real COM Mode



multiple hosts' Real COM drivers open the port at the same time, the COM driver only provides a pure data tunnel—no control ability. The serial port parameters will use firmware settings instead of depending on your application program (AP).

Application software that is based on the COM driver will receive a driver response of "success" when the software uses any of the Win32 API functions. The firmware will only send data back to the driver on the host.

Data will be sent first-in-first-out when data comes into the CN2600 from the Ethernet interface.

ATTENTION

When **Max connection** is greater than 1, the CN2600 will use a multi connection application (i.e., 2 to 8 hosts are allowed access to the port at the same time). When using a multi connection application, the CN2600 will use the serial communication parameters as defined here in the web console, and all hosts connected to the port must use identical serial settings. If one of the hosts opens the COM port with different serial settings, data will not be transmitted properly.

Ignore jammed IP (default=No): This option determines how the port will proceed if multiple hosts are connected and one or more of the hosts stops responding as the port is transmitting data. If you select **No**, the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select **Yes**, the port will ignore the host that stopped responding and continue data transmission to the other hosts.

Allow driver control (default=No): This option determines how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. If **No** is selected, driver control commands will be ignored. If **Yes** is selected, control commands will be accepted, with the most recent command received taking precedence.

Connection goes down (default=always high): You can configure what happens to the RTS and DTR signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent through the serial port. Use **goes low** if you want the RTS and DTR signal to change their state to low when the Ethernet connection goes down. Use **always high** if you do not want the Ethernet connection status to affect the RTS or DTR signals.

Packet length (default=0): The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and Delimiter 2 (default=None): When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.

ATTENTION

In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the CN2600 will still pack and send the data when the amount of data exceeds 1 KB.

Delimiter process (default=Do Nothing): The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.

- Do Nothing: Data in the buffer will be transmitted when the delimiter is received.
- Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.
- Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.
- Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted.

Force transmit (default=0 ms): This parameter defines how large a gap in serial communication the CN2600 will allow before packing the serial data in its internal buffer for network transmission.

As data is received through the serial port, it is stored by the CN2600 in the internal buffer. The CN2600 transmits data stored in the buffer via TCP/IP, but only when the internal buffer is full or as specified by the force transmit time. When set to 0, the force transmit time is disabled, and transmission is determined solely by the data in the internal buffer. At 1 to 65535, the TCP/IP protocol software will pack the serial data received after there is a gap in serial communication that exceeds the specified force transmit time.

The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is

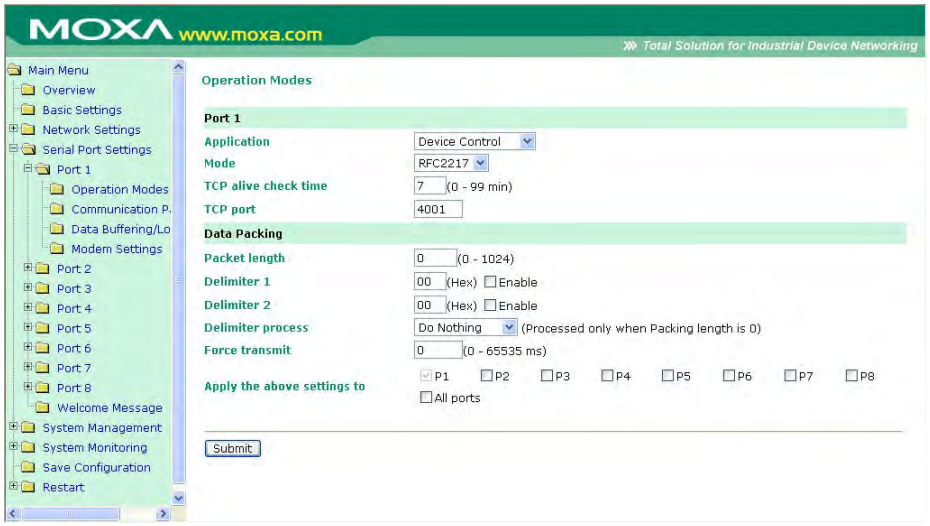
(10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms.

Therefore, you should set the force transmit time to be larger than 8.3 ms, so in this case, it must

be greater than or equal to 10 ms.

If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the CN2600's internal buffer size (1 KB per port).

RFC2217 Mode



TCP alive check time (default=7 min): This field specifies how long the CN2600 will wait for a response to "keep alive" packets before closing the TCP connection. The CN2600 checks connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the CN2600 will force the existing TCP connection to close. For socket and device control modes, the CN2600 will listen for another TCP connection from another host after closing the connection. If **TCP alive check time** is set to **0,** the TCP connection will remain open even if there is no response to the "keep alive" packets.

TCP port (default=4001): This is the TCP port number assignment for the serial port on the CN2600. It is the port number that the serial port uses to listen to connections, and that other devices must use to contact the serial port. To avoid conflicts with well known TCP ports, the default is set to 4001.

Packet length (default=0): The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and Delimiter 2 (default=None): When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to indicate when data should be sent.

ATTENTION

In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the CN2600 will still pack and send the data when the amount of data exceeds 1 KB.

Delimiter process (default=Do Nothing): The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.

- Do Nothing: Data in the buffer will be transmitted when the delimiter is received.
- Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.
- Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.
- Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted.

Force transmit (default=0 ms): This parameter defines how large a gap in serial communication the CN2600 will allow before packing the serial data in its internal buffer for network transmission.

As data is received through the serial port, it is stored by the CN2600 in the internal buffer. The CN2600 transmits data stored in the buffer via TCP/IP, but only when the internal buffer is full or as specified by the force transmit time. When set to 0, the force transmit time is disabled, and transmission is determined solely by the data in the internal buffer. At 1 to 65535, the TCP/IP protocol software will pack the serial data received after there is a gap in serial communication that exceeds the specified force transmit time.

The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is

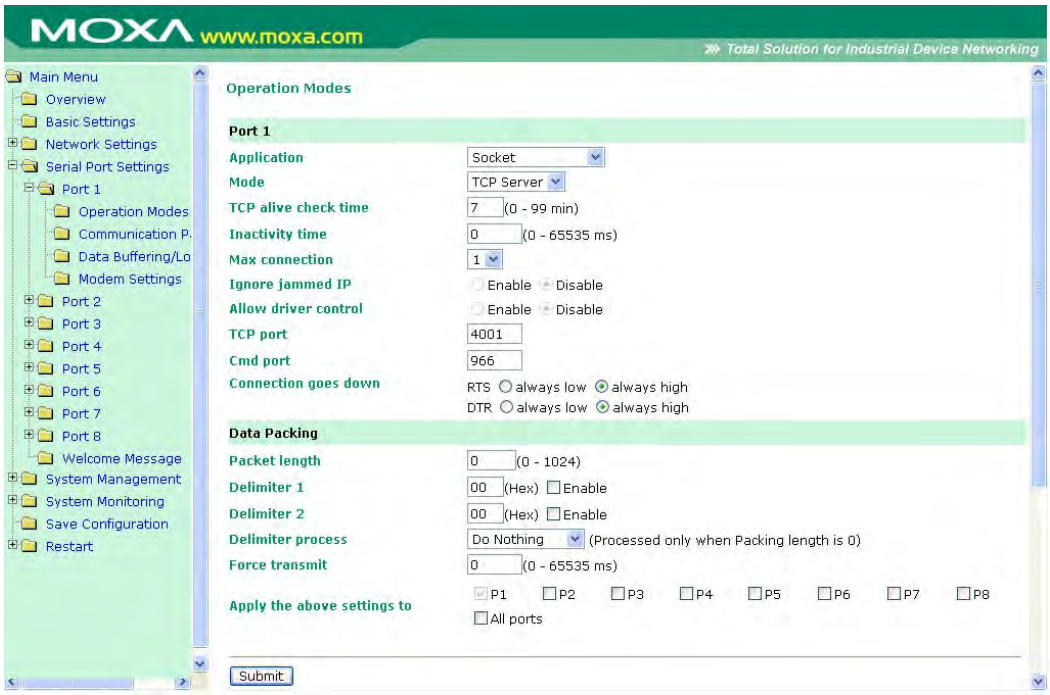
(10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms.

Therefore, you should set the force transmit time to be larger than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.

If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the CN2600's internal buffer size (1 KB per port).

Socket Applications

TCP Server Mode



TCP alive check time (default=7 min): This field specifies how long the CN2600 will wait for a response to "keep alive" packets before closing the TCP connection. The CN2600 checks connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the CN2600 will force the existing TCP connection to close. For socket and device control modes, the CN2600 will listen for another TCP connection from another host after closing the connection. If **TCP alive check time** is set to **0,** the TCP connection will remain open even if there is no response to the "keep alive" packets.

Inactivity time (default=0 ms): This field specifies how long the CN2600 will wait for incoming and outgoing data through the serial port before closing the TCP connection. The TCP connection is closed if there is no incoming or outgoing data through the serial port for the specified **Inactivity time**. If this field is set to **0**, the TCP connection is kept active until a connection close request is received.

ATTENTION

If used, the **Inactivity time** setting should be greater than the **Force transmit** time. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.

Max connection (default=1): This field is used if you need to receive data from different hosts simultaneously. When set to 1, only a single host may open the TCP connection to the serial port. When set to 2 or greater, up to the specified number of hosts may open this port at the same time. When multiple hosts establish a TCP connection to the serial port at the same time, the CN2600 will duplicate the serial data and transmit it to all the hosts. Ethernet data is sent on a first-in first-out basis to the serial port when data comes into the CN2600 from the Ethernet interface.

Ignore jammed IP (default=No): This option determines how the port will proceed if multiple hosts are connected and one or more of the hosts stops responding as the port is transmitting data. If you select **No**, the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select **Yes**, the port will ignore the host that stopped responding and continue data transmission to the other hosts.

Allow driver control (default=No): This option determines how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. If **No** is selected, driver control commands will be ignored. If **Yes** is selected, control commands will be accepted, with the most recent command received taking precedence.

TCP port (default=4001): This is the TCP port number assignment for the serial port on the CN2600. It is the port number that the serial port uses to listen to connections, and that other devices must use to contact the serial port. To avoid conflicts with well known TCP ports, the default is set to 4001.

Command port (default=966): The Command port is the TCP port for listening to SSDK commands from the host. In order to prevent a TCP port conflict with other applications, the user can set the Command port to another port if needed.

Packet length (default=0): The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and Delimiter 2 (default=None): When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to indicate when data should be sent.

ATTENTION

In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the CN2600 will still pack and send the data when the amount of data exceeds 1 KB.

Delimiter process (default=Do Nothing): The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.

- Do Nothing: Data in the buffer will be transmitted when the delimiter is received.
- Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.
- Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.
- Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted.

Force transmit (default=0 ms): This parameter defines how large a gap in serial communication the CN2600 will allow before packing the serial data in its internal buffer for network transmission.

As data is received through the serial port, it is stored by the CN2600 in the internal buffer. The CN2600 transmits data stored in the buffer via TCP/IP, but only when the internal buffer is full or

as specified by the force transmit time. When set to 0, the force transmit time is disabled, and transmission is determined solely by the data in the internal buffer. At 1 to 65535, the TCP/IP protocol software will pack the serial data received after there is a gap in serial communication that exceeds the specified force transmit time.

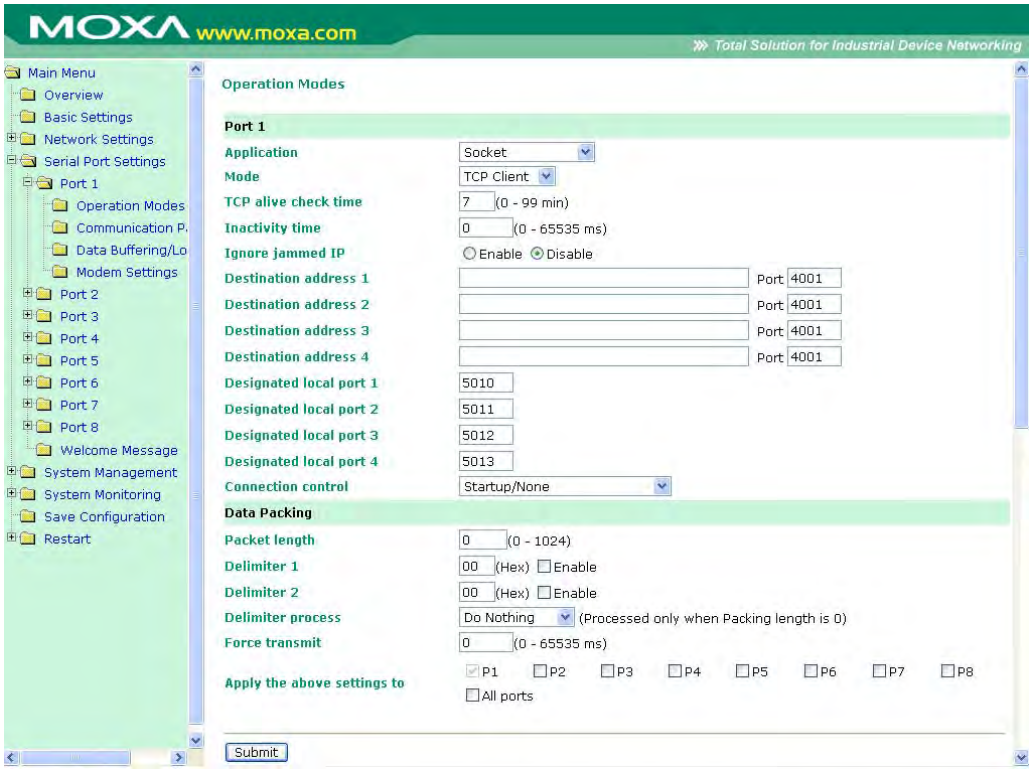
The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is

(10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms.

Therefore, you should set the force transmit time to be larger than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.

If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the CN2600's internal buffer size (1 KB per port).

TCP Client Mode



TCP alive check time (default=7 min): This field specifies how long the CN2600 will wait for a response to "keep alive" packets before closing the TCP connection. The CN2600 checks connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the CN2600 will force the existing TCP connection to close. For socket and device control modes, the CN2600 will listen for another TCP connection from another host after closing the connection. If **TCP alive check time** is set to **0,** the TCP connection will remain open even if there is no response to the "keep alive" packets.

Inactivity time (default=0 ms): This field specifies how long the CN2600 will wait for incoming and outgoing data through the serial port before closing the TCP connection. The TCP connection

is closed if there is no incoming or outgoing data through the serial port for the specified **Inactivity time**. If this field is set to **0**, the TCP connection is kept active until a connection close request is received.

ATTENTION

Inactivity time should at least be set larger than that of **Force transmit** time. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.

ATTENTION

Inactivity time is ONLY active when **Connection Control** (see below) is set to **Any character/Inactivity time.**

Ignore jammed IP (default=No): This option determines how the port will proceed if multiple hosts are connected and one or more of the hosts stops responding as the port is transmitting data. If you select **No**, the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select **Yes**, the port will ignore the host that stopped responding and continue data transmission to the other hosts.

Destination address 1 through **4** (default=None): Specifying an IP address allows the CN2600 to connect actively to the remote host. At least one destination must be provided.

TCP port (default=4001): This is the TCP port number assignment for the serial port on the CN2600. It is the port number that the serial port uses to listen to connections, and that other devices must use to contact the serial port. To avoid conflicts with well known TCP ports, the default is set to 4001.

ATTENTION

Up to 4 connections can be established between the CN2600 and hosts. The connection speed or throughput may be low if any one of the four connections is slow, since the one slow connection will slow down the other 3 connections.

ATTENTION

The **Destination IP** address parameter can be the IP address, domain name, or the name defined in the host table. For some applications, the user may need to send the data actively to the remote destination domain name.

Designated local port 1 through **4** (default=5010 through 5013): Use these fields to specify the designated local ports.

Connection control (default=Startup/None): This setting determines the parameters under which a TCP connection is established or disconnected. The different options are given in the following table. In general, both the Connect condition and Disconnect conditions are given.

Option	Description
Startup/None (default)	A TCP connection will be established on startup, and will remain active indefinitely.
Any Character/None	A TCP connection will be established when any character is received from the serial interface, and will remain active indefinitely.
Any Character/ Inactivity Time	A TCP connection will be established when any character is received from the serial interface, and will be disconnected when **Inactivity time** is reached.
DSR On/DSR Off	A TCP connection will be established when a DSR "On" signal is received, and will be disconnected when a DSR "Off" signal is received.
DSR On/None	A TCP connection will be established when a DSR signal of NPort is "On", and will remain active indefinitely.
DCD On/DCD Off	A TCP connection will be established when a DCD "On" signal is received, and will be disconnected when a DCD "Off" signal is received.
DCD On/None	A TCP connection will be established when a DCD "On" signal is received, and will remain active indefinitely.

Packet length (default=0): This field refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and Delimiter 2 (default=None): When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to indicate when data should be sent.

ATTENTION

In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the CN2600 will still pack and send the data when the amount of data exceeds **1 KB**.

Delimiter process (default=Do Nothing): The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.

- Do Nothing: Data in the buffer will be transmitted when the delimiter is received.
- Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.
- Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.
- Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted.

Force transmit (default=0 ms): This parameter defines how large a gap in serial communication the CN2600 will allow before packing the serial data in its internal buffer for network transmission.

As data is received through the serial port, it is stored by the CN2600 in the internal buffer. The CN2600 transmits data stored in the buffer via TCP/IP, but only when the internal buffer is full or as specified by the force transmit time. When set to 0, the force transmit time is disabled, and transmission is determined solely by the data in the internal buffer. At 1 to 65535, the TCP/IP protocol software will pack the serial data received after there is a gap in serial communication that exceeds the specified force transmit time.

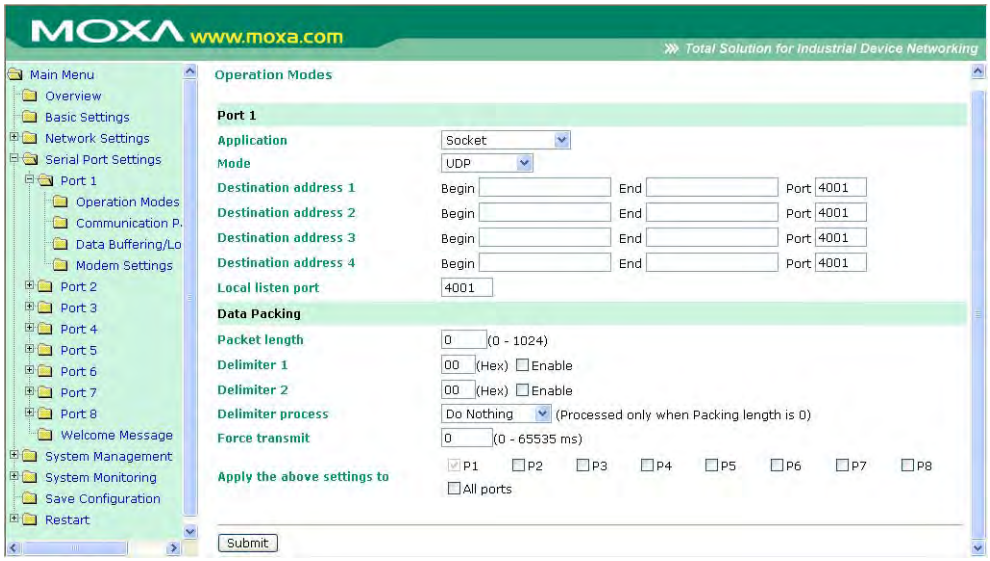
The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is

(10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms.

Therefore, you should set the force transmit time to be larger than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.

If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the CN2600's internal buffer size (1 KB per port).

UDP Mode



Destination address 1 through **4** (default=None): In UDP mode, you may specify up to 4 ranges of IP addresses for the serial port to connect to. At least one destination range must be provided.

ATTENTION

The maximum selectable IP address range is 64 addresses. However, when using multi-unicast, you may enter IP addresses of the form *xxx.xxx.xxx*.**255** in the **Begin** field. For example, enter **192.127.168.255** to allow the CN2600 to broadcast UDP packets to all hosts with IP addresses between 192.127.168.1 and 192.127.168.254.

Local listen port (default=4001): This is the UDP port that the CN2600 listens to and that other devices must use to contact the CN2600. To avoid conflicts with well known UDP ports, the default is set to 4001.

Packet length (default=0): The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and Delimiter 2 (default=None): When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to indicate when data should be sent.

ATTENTION

In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the CN2600 will still pack and send the data when the amount of data exceeds **1 KB**.

Delimiter process (default=Do Nothing): The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.

- Do Nothing: Data in the buffer will be transmitted when the delimiter is received.
- Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.
- Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.
- Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted.

Force transmit (default=0 ms): This parameter defines how large a gap in serial communication the CN2600 will allow before packing the serial data in its internal buffer for network transmission.

As data is received through the serial port, it is stored by the CN2600 in the internal buffer. The CN2600 transmits data stored in the buffer via TCP/IP, but only when the internal buffer is full or as specified by the force transmit time. When set to 0, the force transmit time is disabled, and transmission is determined solely by the data in the internal buffer. At 1 to 65535, the TCP/IP protocol software will pack the serial data received after there is a gap in serial communication that exceeds the specified force transmit time.

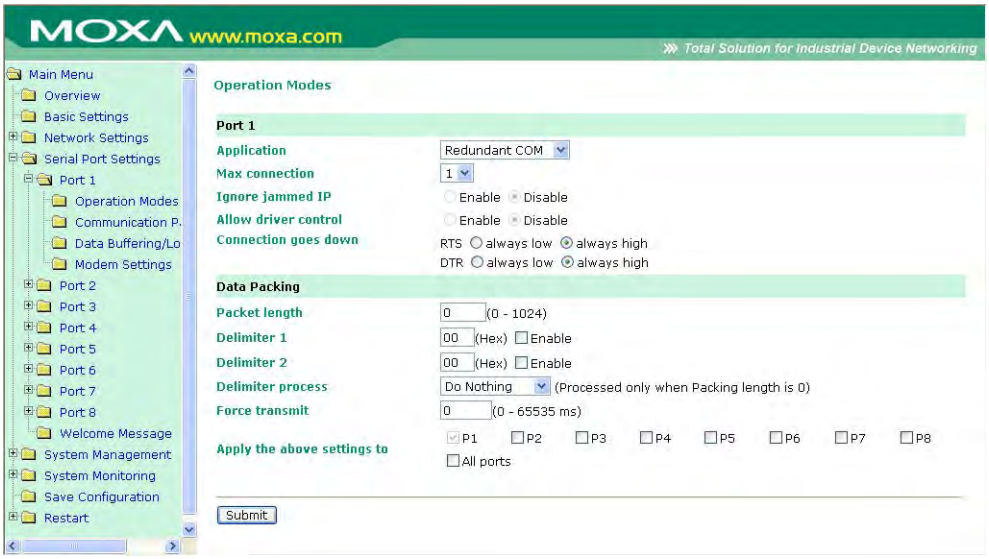
The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is

(10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms.

Therefore, you should set the force transmit time to be larger than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.

If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the CN2600's internal buffer size (1 KB per port).

Redundant COM



Max connection (default=1): This field is used if you need to receive data from different hosts simultaneously. When set to 1, only one specific host can access this port of the CN2600, and the Redundant COM driver on that host will have full control over the port. When set to 2 or greater, up to the specified number of hosts' Redundant COM drivers may open this port at the same time. When multiple hosts' Redundant COM drivers open the port at the same time, the COM driver only provides a pure data tunnel—no control ability. The serial port parameters will use firmware settings instead of depending on your application program (AP).

Application software that is based on the COM driver will receive a driver response of "success" when the software uses any of the Win32 API functions. The firmware will only send data back to the driver on the host.

Data will be sent first-in-first-out when data comes into the CN2600 from the Ethernet interface.

ATTENTION

When **Max connection** is greater than 1, the CN2600 will use a multi connection application (i.e., 2 to 4 hosts are allowed access to the port at the same time). When using a multi connection application, the CN2600 will use the serial communication parameters as defined here in the web console, and all hosts connected to the port must use identical serial settings. If one of the hosts opens the COM port with different serial settings, data will not be transmitted properly.

Ignore jammed IP (default=No): This option determines how the port will proceed if multiple hosts are connected and one or more of the hosts stops responding as the port is transmitting data. If you select **No**, the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select **Yes**, the port will ignore the host that stopped responding and continue data transmission to the other hosts.

Allow driver control (default=No): This option determines how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. If **No** is selected, driver control commands will be ignored. If **Yes** is selected, control commands will be accepted, with the most recent command received taking precedence.

Connection goes down (default=always high): You can configure what happens to the RTS and DTR signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent through the serial port. Use **goes low** if you want the RTS and DTR signal to change their state to low when the Ethernet connection goes down. Use **always high** if you do not want the Ethernet connection status to affect the RTS or DTR signals.

Packet length (default=0): The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and Delimiter 2 (default=None): When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.

ATTENTION

In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the CN2600 will still pack and send the data when the amount of data exceeds 1 KB.

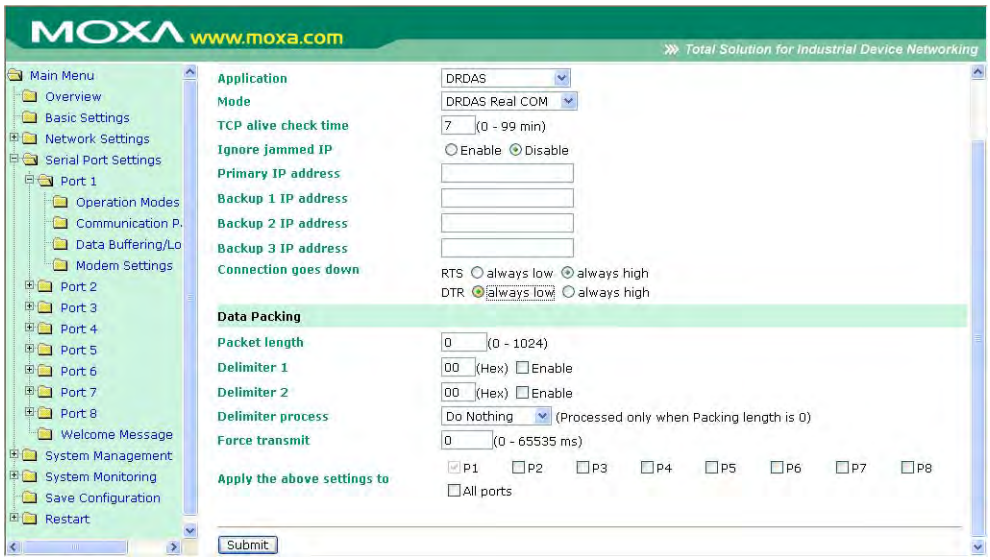
Delimiter process (default=Do Nothing): The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.

- Do Nothing: Data in the buffer will be transmitted when the delimiter is received.
- Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.
- Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.
- Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted.

Force transmit (default=0 ms): This parameter defines how large a gap in serial communication the CN2600 will allow before packing the serial data in its internal buffer for network transmission.

DRDAS

DRDAS Real COM



TCP alive check time (default=7 min): This field specifies how long the CN2600 will wait for a response to "keep alive" packets before closing the TCP connection. The CN2600 checks connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the CN2600 will force the existing TCP connection to close. For socket and device control modes, the CN2600 will listen for another TCP connection from another host after closing the connection. If **TCP alive check time** is set to **0**, the TCP connection will remain open and will not send any "keep alive" packets.

Ignore jammed IP (default=No): This option determines how the port will proceed if multiple hosts are connected and one or more of the hosts stops responding as the port is transmitting data. If you select **No**, the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select **Yes**, the port will ignore the host that stopped responding and continue data transmission to the other hosts.

Primary IP address The primary host's IP address.

If left blank, then every host on the network cannot access the serial port.

Backup 1 IP address Backup host's IP address

Backup 2 IP address Backup host's IP address

Backup 3 IP address Backup host's IP address

Connection goes down (default=always high): You can configure what happens to the RTS and DTR signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent through the serial port. Use **goes low** if you want the RTS and DTR signal to change their state to low when the Ethernet connection goes down. Use **always high** if you do not want the Ethernet connection status to affect the RTS or DTR signals.

Packet length (default=0): The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter

settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and Delimiter 2 (default=None): When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.

ATTENTION

In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the CN2600 will still pack and send the data when the amount of data exceeds 1 KB.

Delimiter process (default=Do Nothing): The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.

- Do Nothing: Data in the buffer will be transmitted when the delimiter is received.
- Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.
- Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.
- Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted.

Force transmit (default=0 ms): This parameter defines how large a gap in serial communication the CN2600 will allow before packing the serial data in its internal buffer for network transmission..

As data is received through the serial port, it is stored by the CN2600 in the internal buffer. The CN2600 transmits data stored in the buffer via TCP/IP, but only when the internal buffer is full or as specified by the force transmit time. When set to 0, the force transmit time is disabled, and transmission is determined solely by the data in the internal buffer. At 1 to 65535, the TCP/IP protocol software will pack the serial data received after there is a gap in serial communication that exceeds the specified force transmit time.

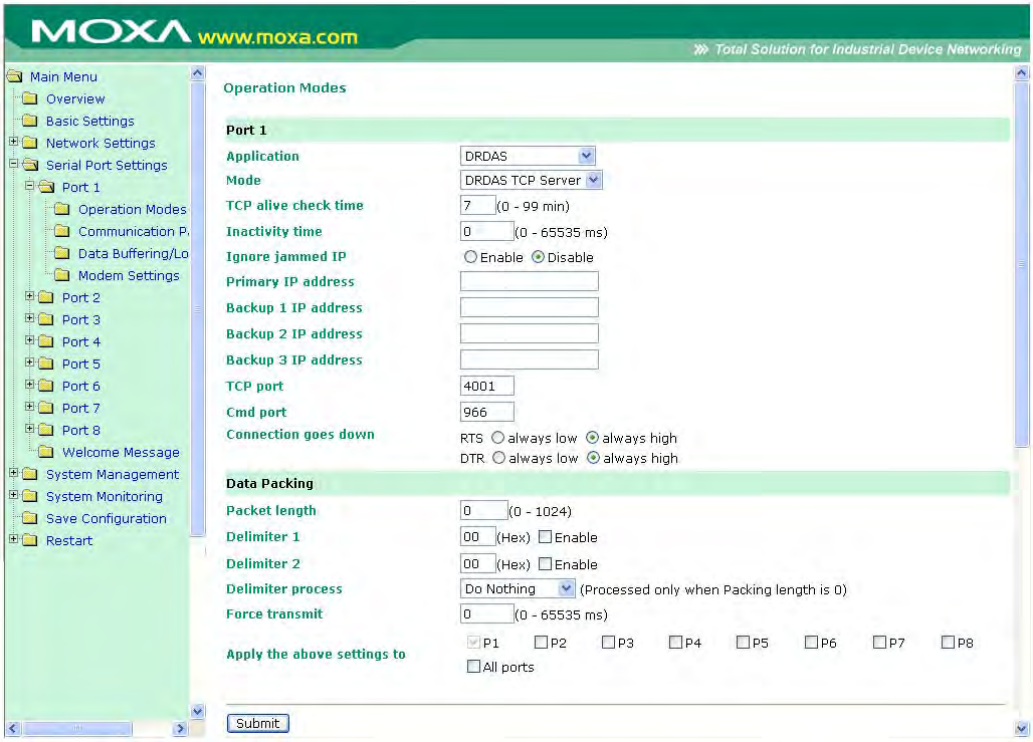
The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is

(10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms.

Therefore, you should set the force transmit time to be larger than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.

If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the CN2600's internal buffer size (1 KB per port).

DRDAS TCP Server



TCP alive check time (default=7 min): This field specifies how long the CN2600 will wait for a response to "keep alive" packets before closing the TCP connection. The CN2600 checks connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the CN2600 will force the existing TCP connection to close. For socket and device control modes, the CN2600 will listen for another TCP connection from another host after closing the connection. If **TCP alive check time** is set to **0**, the TCP connection will remain open even if there is no response to the "keep alive" packets.

Inactivity time (default=0 ms): This field specifies how long the CN2600 will wait for incoming and outgoing data through the serial port before closing the TCP connection. The TCP connection is closed if there is no incoming or outgoing data through the serial port for the specified **Inactivity time**. If this field is set to **0**, the TCP connection is kept active until a connection close request is received.

Ignore jammed IP (default=No): This option determines how the port will proceed if multiple hosts are connected and one or more of the hosts stops responding as the port is transmitting data. If you select **No**, the port will wait until the data has been transmitted successfully to all hosts before transmitting the next group of data. If you select **Yes**, the port will ignore the host that stopped responding and continue data transmission to the other hosts.

Primary IP address The primary host's IP address.If left blank, then every host on the network cannot access the serial port.

Backup 1 IP address Backup host's IP address

Backup 2 IP address Backup host's IP address

Backup 3 IP address Backup host's IP address

TCP Port TCP data port number Via the data port, users can retrieve data through the async line.

TCP port command port number Via the command port, users can issue commands across the network to set the line's configuration parameters, such as baudrate, data bits, flow control condition, etc.

Connection goes down (default=always high): You can configure what happens to the RTS and DTR signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent through the serial port. Use **goes low** if you want the RTS and DTR signal to change their state to low when the Ethernet connection goes down. Use **always high** if you do not want the Ethernet connection status to affect the RTS or DTR signals.

Packet length (default=0): The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default of 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and Delimiter 2 (default=None): When Delimiter 1 is enabled, the serial port will clear the buffer and send the data to the Ethernet port when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.

ATTENTION

In order to enable a delimiter, packet length must be set to 0. Delimiter 2 should only be enabled in conjunction with Delimiter 1 and never on its own; otherwise there may be data errors. Even when a delimiter is enabled, the CN2600 will still pack and send the data when the amount of data exceeds 1 KB.

Delimiter process (default=Do Nothing): The Delimiter process field determines how the data is handled when a delimiter is received. Delimiter 1 must be enabled for this field to have effect. If Delimiters 1 and 2 are both enabled, both characters must be received for the delimiter process to take place.

- Do Nothing: Data in the buffer will be transmitted when the delimiter is received.
- Delimiter + 1: Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.
- Delimiter + 2: Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.
- Strip Delimiter: Data in the buffer is first stripped of the delimiter before being transmitted.

Force transmit (default=0 ms): This parameter defines how large a gap in serial communication the CN2600 will allow before packing the serial data in its internal buffer for network transmission.

As data is received through the serial port, it is stored by the CN2600 in the internal buffer. The CN2600 transmits data stored in the buffer via TCP/IP, but only when the internal buffer is full or as specified by the force transmit time. When set to 0, the force transmit time is disabled, and transmission is determined solely by the data in the internal buffer. At 1 to 65535, the TCP/IP protocol software will pack the serial data received after there is a gap in serial communication that exceeds the specified force transmit time.

The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send

a character is 10 bits, and the time required to transfer one character is

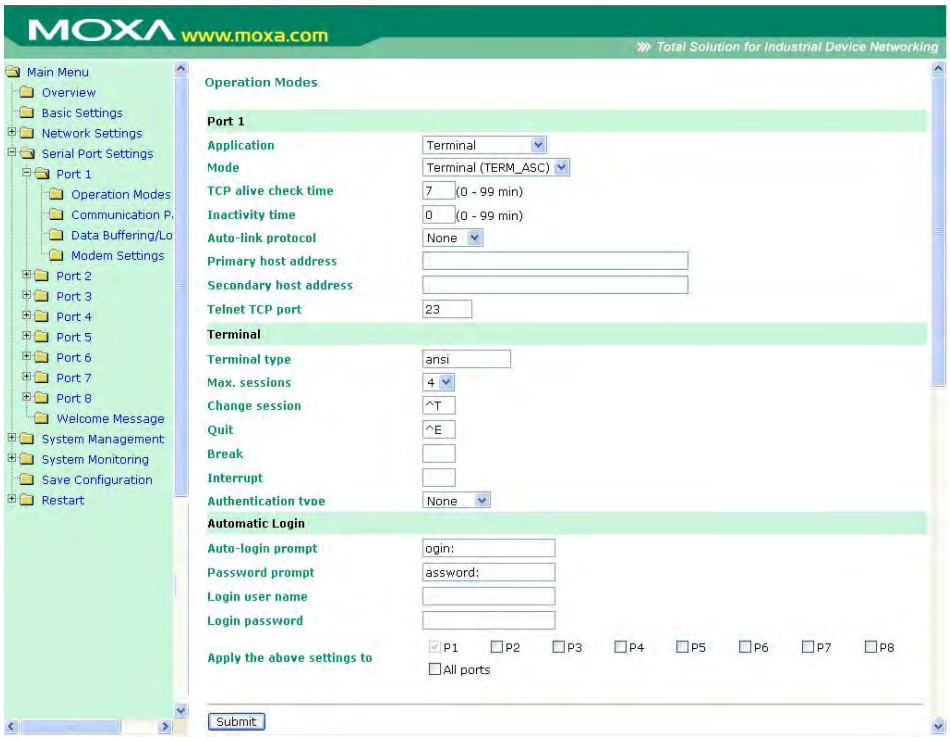
(10 (bits) / 1200 (bits/s)) × 1000 (ms/s) = 8.3 ms.

Therefore, you should set the force transmit time to be larger than 8.3 ms, so in this case, it must be greater than or equal to 10 ms.

If it is necessary to send a series of characters in the same packet, the serial device will need to send that series of characters within the specified force transmit time, and the total length of data must be less than or equal to the CN2600's internal buffer size (1 KB per port).

Terminal Applications

Terminal ASCII (TERM_ASC)



TCP alive check time (default=7 min): This field specifies how long the CN2600 will wait for a response to "keep alive" packets before closing the TCP connection. The CN2600 checks connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the CN2600 will force the existing TCP connection to close. For socket and device control modes, the CN2600 will listen for another TCP connection from another host after closing the connection. If **TCP alive check time** is set to **0,** the TCP connection will remain open even if there is no response to the "keep alive" packets.

Inactivity time (default=0 min): This field specifies how long the CN2600 will wait for incoming and outgoing data through the serial port before closing the TCP connection. The TCP connection is closed if there is no incoming or outgoing data through the serial port for the specified **Inactivity time**. If this field is set to **0**, the TCP connection is kept active until a connection close request is received.

ATTENTION

Inactivity time should at least be set larger than that of **Force transmit** time. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough such that the intended data transfer is completed.

Auto-Link Protocol: If this field is set to **None**, the CN2600 will not connect to the host automatically. If Auto-Link Protocol is set to **Telnet** or **Rlogin**, the CN2600 will connect to the host automatically using the specified protocol.

Primary and **Secondary host address**: If specified, the fields designate permanent hosts to which the terminal will always be connected.

Telnet TCP port (default=23): By default, the Telnet TCP port number is set to 23, which is the default TCP port number for Telnet.

Terminal type (default=ansi): Some older terminal applications may require that the terminal type be transmitted before the connection can be established. You may need to refer to the server's documentation to determine the appropriate terminal type. For most applications, this setting will be unnecessary and will have no effect

Max. Sessions (default=4): This setting allows you to configure the maximum. number of sessions allowed for the serial port.

Change Session (default=(^T)0x14): This field defines the quick key to change a session.

Quit (default=(^E)0x05): This field defines the quick key to quit a session.

Break: This field defines the quick key to send a break signal.

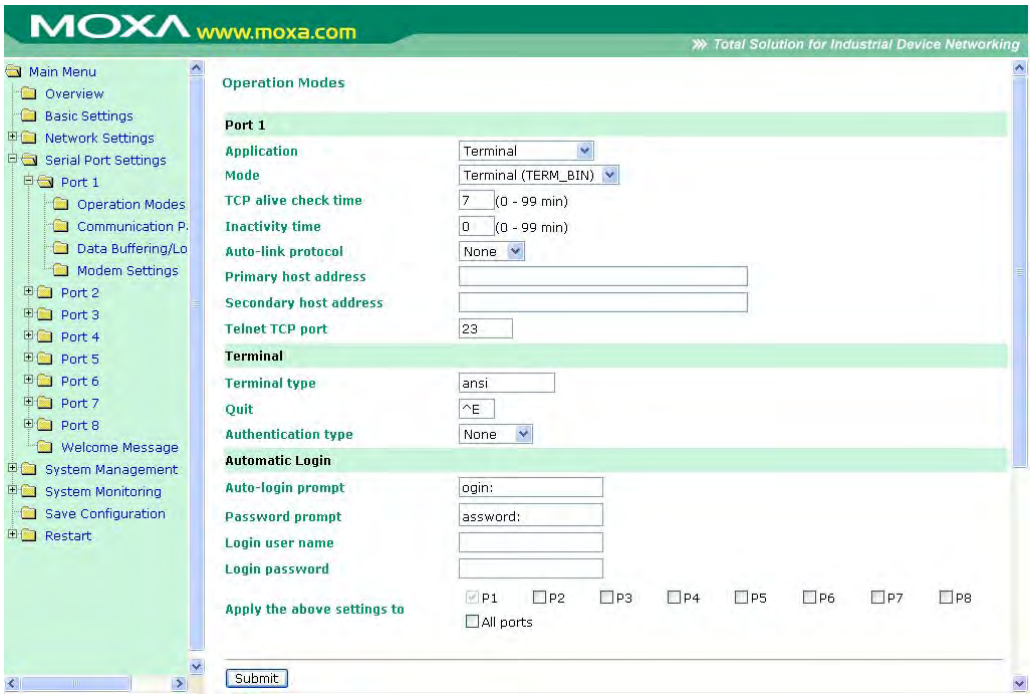
Interrupt: This field defines the quick key for program termination.

Authentication type (default=None): This field allows you to configure the method used, if any, to verify a user's ID and authorization.

Option	Description
Local	Verify the ID against the CN2600 User Table.
RADIUS	Verify the ID against the external RADIUS server.
None	Authentication is not required.

Auto-login prompt (default=ogin:)
Password prompt (default=assword:)
Login user name: Enter the terminal login ID here.
Login password: Enter the password for the terminal login here.

Terminal BIN (TERM_BIN)



Terminal Binary mode can be used to transfer files with XMODEM or ZMODEM. You are only allowed to open one terminal session at a time when in Terminal Binary mode.

TCP alive check time (default=7 min): This field specifies how long the CN2600 will wait for a response to "keep alive" packets before closing the TCP connection. The CN2600 checks connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the CN2600 will force the existing TCP connection to close. For socket and device control modes, the CN2600 will listen for another TCP connection from another host after closing the connection. If **TCP alive check time** is set to **0,** the TCP connection will remain open even if there is no response to the "keep alive" packets.

Inactivity time (default=0 min): This field specifies how long the CN2600 will wait for incoming and outgoing data through the serial port before closing the TCP connection. The TCP connection is closed if there is no incoming or outgoing data through the serial port for the specified **Inactivity time**. If this field is set to **0**, the TCP connection is kept active until a connection close request is received.

ATTENTION

Inactivity time should at least be set larger than that of **Force transmit** time. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.

Auto-Link Protocol: If this field is set to **None**, the CN2600 will not connect to the host automatically. If Auto-Link Protocol is set to **Telnet** or **Rlogin**, the CN2600 will connect to the host automatically using the specified protocol.

Primary and **Secondary host address**: If specified, the fields designate permanent hosts to which the terminal will always be connected.

Telnet TCP port (default=23): By default, the Telnet TCP port number is set to 23, which is the default TCP port number for Telnet.

Terminal type (default=ansi): Some older terminal applications may require that the terminal type be transmitted before the connection can be established. You may need to refer to the server's documentation to determine the appropriate terminal type. For most applications, this setting will be unnecessary and will have no effect

Quit (default=(^E) 0x05): This field configures the quick key used to disconnect the link between the current terminal session and the remote host. It is not necessary for binary communication.

Authentication type (default=None): This field allows you to configure the method used, if any, to verify a user's ID and authorization.

Option	Description
Local	Verify the ID against the CN2600 User Table.
RADIUS	Verify the ID against the external RADIUS server.
None	Authentication is not required.

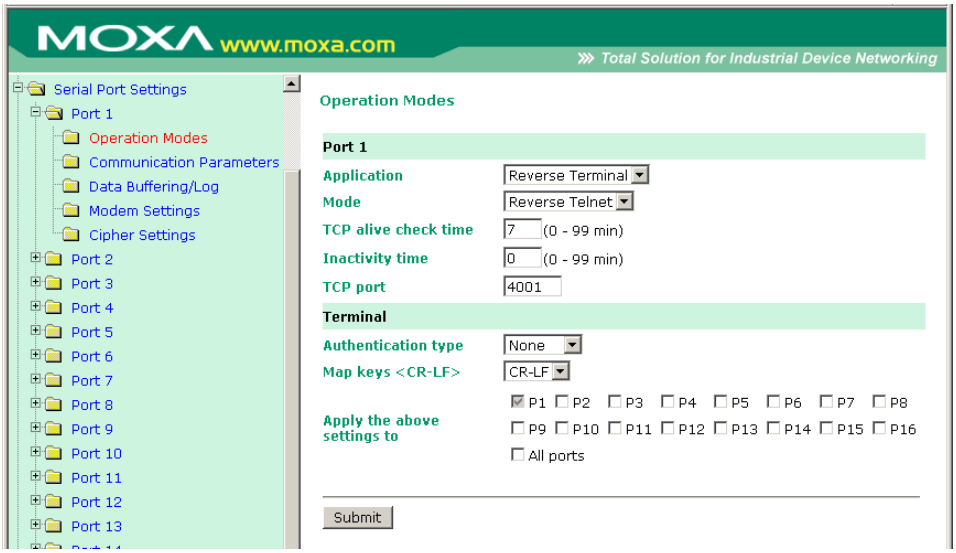
Auto-login prompt (default=ogin:)

Password prompt (default=assword:)

Login user name: Enter the terminal login ID here.

Login password: Enter the password for the terminal login here.

Reverse Terminal



TCP alive check time (default=7 min): This field specifies how long the CN2600 will wait for a response to "keep alive" packets before closing the TCP connection. The CN2600 checks connection status by sending periodic "keep alive" packets. If the remote host does not respond to the packet within the time specified in this field, the CN2600 will force the existing TCP connection to close. For socket and device control modes, the CN2600 will listen for another TCP connection from another host after closing the connection. If **TCP alive check time** is set to **0,** the TCP connection will remain open even if there is no response to the "keep alive" packets.

Inactivity time (default=0 min): This field specifies the idle time setting for auto-disconnection. A setting of 0 min. will cause the port to remain connected even if idle.

TCP port (default=4001): This is the TCP port number assignment for the serial port on the CN2600. It is the port number that the serial port uses to listen to connections, and that other devices must use to contact the serial port. To avoid conflicts with well known TCP ports, the default is set to 4001.

Authentication type (default=None): This field allows you to configure the method used, if any, to verify a user's ID and authorization.

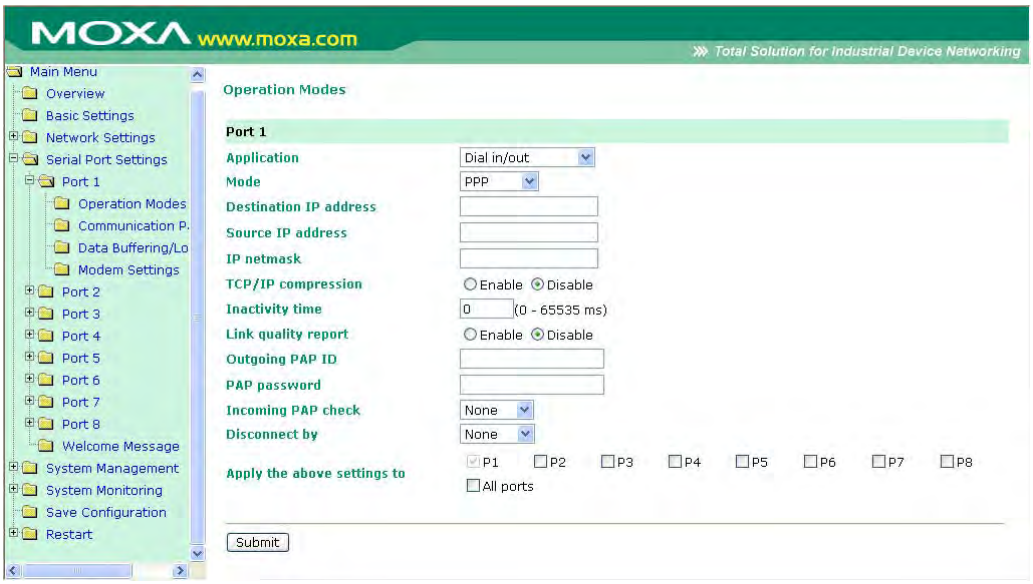
Option	Description
Local	Verify the ID against the CN2600 User Table.
RADIUS	Verify the ID against the external RADIUS server.
None	Authentication is not required.

Map keys <CR-LF> (default=CR-LF): This specifies how the **ENTER** key is mapped from the Ethernet port through the serial port.

Option	Description
<CR-LF>	carriage return + line feed (i.e., the cursor will jump to the next line, and return to the first character of the line)
<CR>	carriage return (i.e., the cursor will return to the first character of the line)
<LF>	line feed (i.e., the cursor will jump to the next line, but not move horizontally)

Dial In/Out Applications

PPP Mode



PPP provides standard PPP service for both dial-in and dial-out.

Destination IP address: This is the IP address of the remote dial-in/ dial-out server.

Source IP address: The Source IP address is IP address assigned to this serial port.

IP netmask: The IP netmask defines the netmask, also known as the subnet mask, for the PPP connection

TCP/IP compression (default=No): The setting of this field depends on whether the remote user's application requests compression.

Inactivity time (default=0 ms): This field specifies the idle time setting for auto-disconnection. A setting of 0 ms will cause the port to remain connected even if idle.

Link quality report (default=No): Setting this field to **Yes** allows the CN2600 to disconnect a connection if the link noise exceeds a certain threshold.

Outgoing PAP ID: This is the dial-out user ID account.

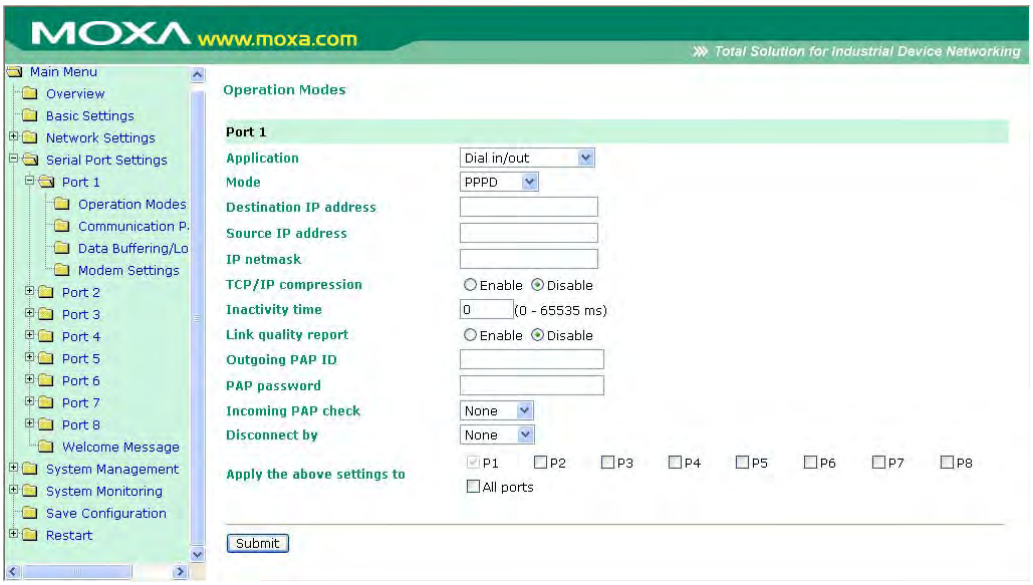
PAP password: This is the dial-out user password.

Incoming PAP check (default=None): This field allows you to configure the method used, if any, to verify a user's ID and authorization.

Option	Description
Local	Verify the ID against the CN2600 User Table.
RADIUS	Verify the ID against the external RADIUS server.
None	Authentication is not required.

Disconnect by (default=None): If this field is set as **DCD-off**, the connection will be disconnected when the DCD signal is off. If this field is set as **DSR-off**, the connection will be disconnected when the DSR signal is off.

PPPD Mode



PPPD (PPP on demand) is used for dial-in services, since it provides PPP services only when receiving a request from a remote PC.

Destination IP address: This is the IP address of the remote dial-in/ dial-out server.

Source IP address: The Source IP address is IP address assigned to this serial port.

IP netmask: The IP netmask defines the netmask, also known as the subnet mask, for the PPP connection

TCP/IP compression (default=No): The setting of this field depends on whether the remote user's application requests compression.

Inactivity time (default=0 ms): This field specifies the idle time setting for auto-disconnection. A setting of 0 ms will cause the port to remain connected even if idle.

Link quality report (default=No): Setting this field to **Yes** allows the CN2600 to disconnect a connection if the link noise exceeds a certain threshold.

Outgoing PAP ID: This is the dial-out user ID account.

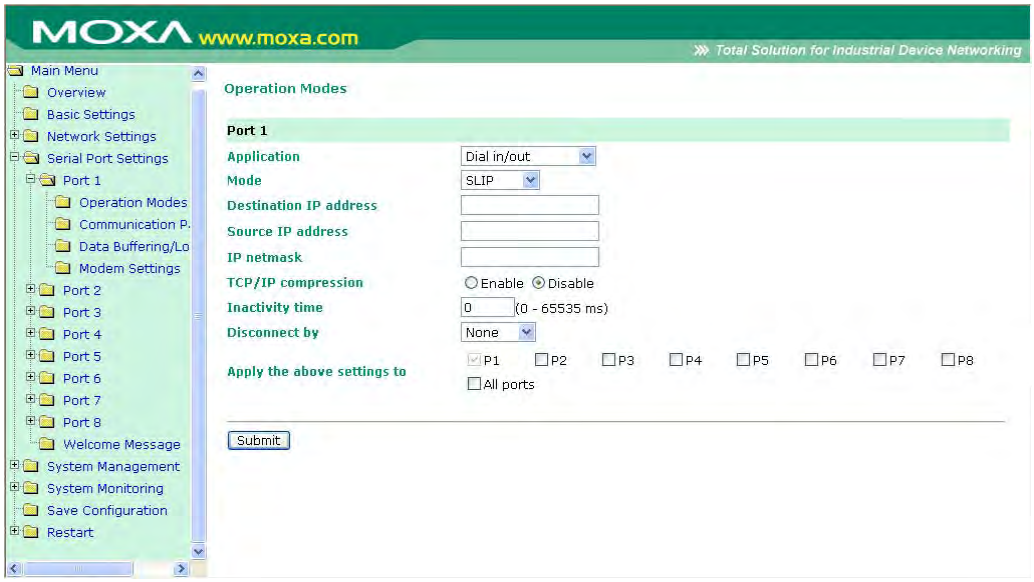
PAP password: This is the dial-out user password.

Incoming PAP check (default=None): This field allows you to configure the method used, if any, to verify a user's ID and authorization.

Option	Description
Local	Verify the ID against the CN2600 User Table.
RADIUS	Verify the ID against the external RADIUS server.
None	Authentication is not required.

Disconnect by (default=None): If this field is set as **DCD-off**, the connection will be disconnected when the DCD signal is off. If this field is set as **DSR-off**, the connection will be disconnected when the DSR signal is off.

SLIP Mode



SLIP provides standard SLIP service for both dial-in and dial-out.

Destination IP address: This is the IP address of the remote dial-in/ dial-out server.

Source IP address: The Source IP address is IP address assigned to this serial port.

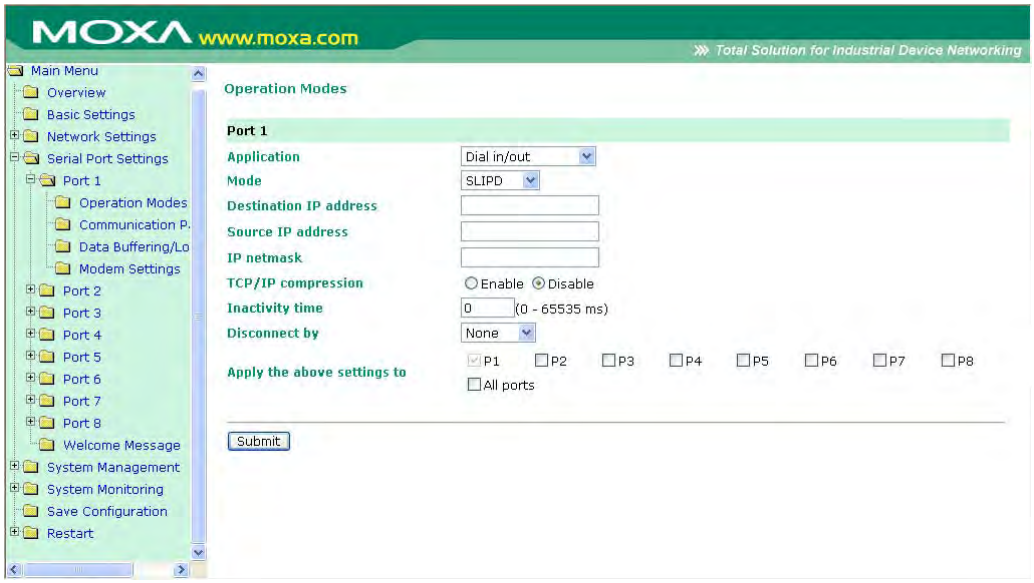
IP netmask: The IP netmask defines the netmask, also known as the subnet mask, for the SLIP connection

TCP/IP compression (default=No): The setting of this field depends on whether the remote user's application requests compression.

Inactivity time (default=0 ms): This field specifies the idle time setting for auto-disconnection. A setting of 0 ms will cause the port to remain connected even if idle.

Disconnect by (default=None): If this field is set as **DCD-off**, the connection will be disconnected when the DCD signal is off. If this field is set as **DSR-off**, the connection will be disconnected when the DSR signal is off.

SLIPD Mode



SLIPD (SLIP on demand) is used for dial-in services, since it provides SLIP services only when receiving a request from a remote PC.

Destination IP address: This is the IP address of the remote dial-in/ dial-out server.

Source IP address: The Source IP address is IP address assigned to this serial port.

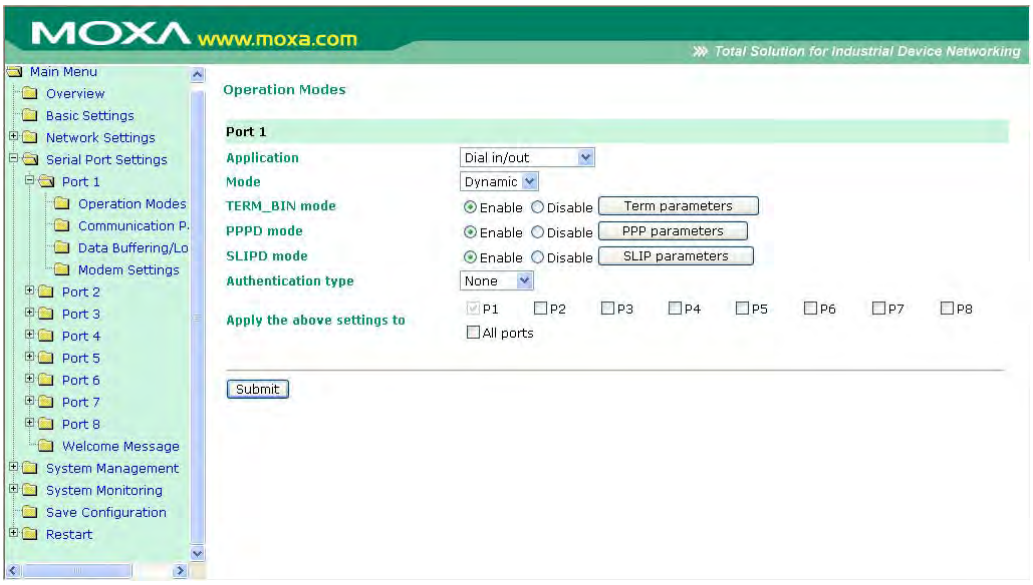
IP netmask: The IP netmask defines the netmask, also known as the subnet mask, for the SLIP connection

TCP/IP compression (default=No): The setting of this field depends on whether the remote user's application requests compression.

Inactivity time (default=0 ms): This field specifies the idle time setting for auto-disconnection. A setting of 0 ms will cause the port to remain connected even if idle.

Disconnect by (default=None): If this field is set as **DCD-off**, the connection will be disconnected when the DCD signal is off. If this field is set as **DSR-off**, the connection will be disconnected when the DSR signal is off.

Dynamic Mode

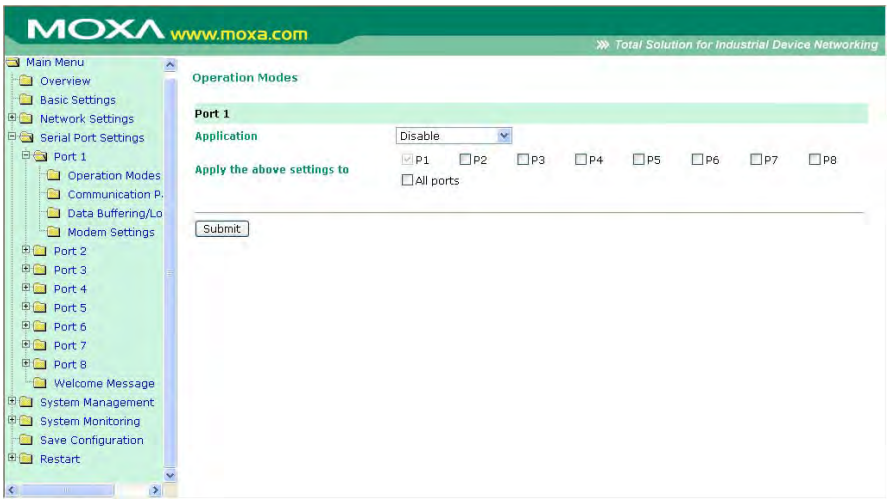


Dynamic mode integrates PPPD, SLIPD, and Terminal dial-in services. Dynamic mode automatically detects which remote connection mode is being used, and provides corresponding services. You can individually enable/disable PPP/SLIP/Terminal services by selecting Yes or No next to the corresponding option. Yes will enable that type of service; No will disable it.

Authentication type (default=None): This field allows you to configure the method used, if any, to verify a user's ID and authorization.

Option	Description
Local	Verify the ID against the CN2600 User Table.
RADIUS	Verify the ID against the external RADIUS server.
None	Authentication is not required.

Disabled Mode



When the **Application** is set to **Disable**, the relevant port will be disabled.

7

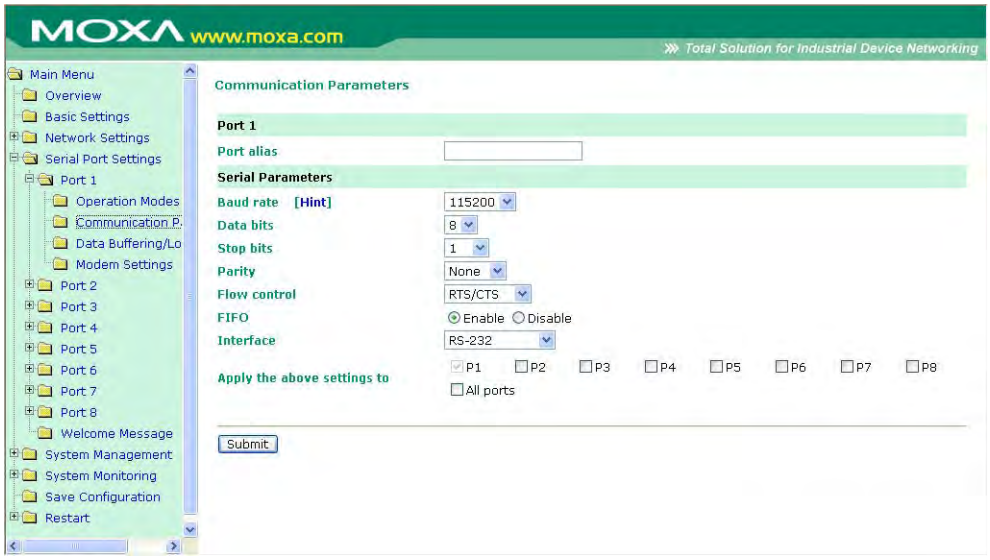
Additional Serial Port Settings

In this chapter, we describe additional serial port settings on the CN2600. The same configuration options are also available through the telnet and serial console.

This chapter covers the following topics:

- **Port Communication Parameters**
- **Serial Parameters**
- **Port Data Buffering/Log**
- **Port Modem Settings**
- **Welcome Message**

Port Communication Parameters



Port alias: This optional field allows you to assign an alias to a port for easier identification.

Serial Parameters

ATTENTION

The serial parameters for the each serial port on the CN2600 should match the parameters used by the connected serial device. You may need to refer to your serial device's user's manual to determine the appropriate serial communication parameters.

Baud rate (default=115200 bps): This field configures the port's baudrate. Select one of the standard baudrates from the dropdown box, or select **Other** and then type the desired baudrate in the input box.

ATTENTION

If the port requires a special baudrate that is not listed, such as 500000 bps, you may can select the **Other** option and enter the desired baudrate into the text box. The CN2600 will automatically calculate the closest supported baudrate. The margin for error will be less than 1.7% for all baudrates under 921600 bps.

Data bits (default=8): This field configures the data bits parameter. Note: If data bits is set to 5 bits, stop bits will automatically be set to 2 bits.

Stop bits (default=1): This field configures the stop bits parameter. Note: If data bits is set to 5 bits, stop bits will automatically be set to 1.5 bits.

Parity (default=None): This field configures the parity parameter.

Flow control (default=RTS/CTS): This field configures the flow control type.

FIFO (default=Enable): This field enables or disables the 128-byte FIFO buffer. The CN2600 provides FIFO buffers for each serial port, for both the Tx and Rx signals. Note, however, that you

should disable the port's FIFO setting if the attached serial device does not have a FIFO buffer of its own. This is because a serial device that does not have its own buffer may not be able to keep up with data sent from the CN2600's FIFO buffer.

Interface (default=RS-232): You may configure the serial interface to RS-232, RS-422, RS-485 2-wire, or RS-485 4-wire.

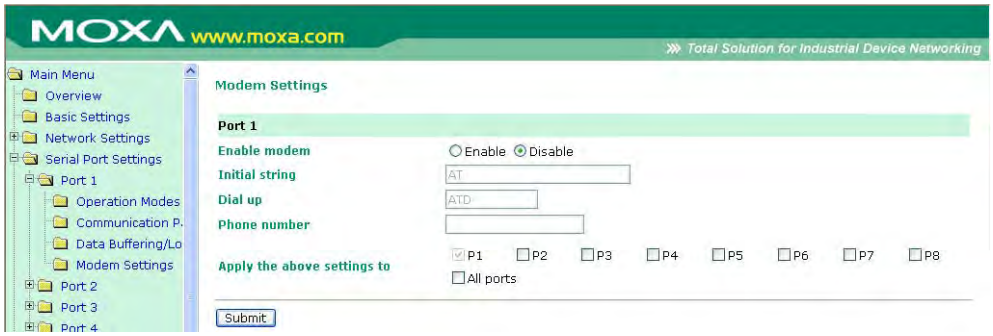
Port Data Buffering/Log

The CN2600 supports port buffering to prevent the loss of serial data when the Ethernet connection is down. Port buffering can be used in TCP Server mode, TCP Client mode, and Pair Connection mode. For other modes, the port buffering settings will have no effect.

Port buffering enable (default=No): You may enable port buffering by setting this field to **Yes**.

Serial data logging enable (default=No): If this field is set to Yes, the CN2600 will store data logs on the system RAM for all serial ports. Note that this data is not saved when the CN2600 is powered off. Each serial port is allotted 128 KB to store that port's log file.

Port Modem Settings



Modem settings are used for the Dial In/Out modes. These settings will have no effect on ports configured for other modes.

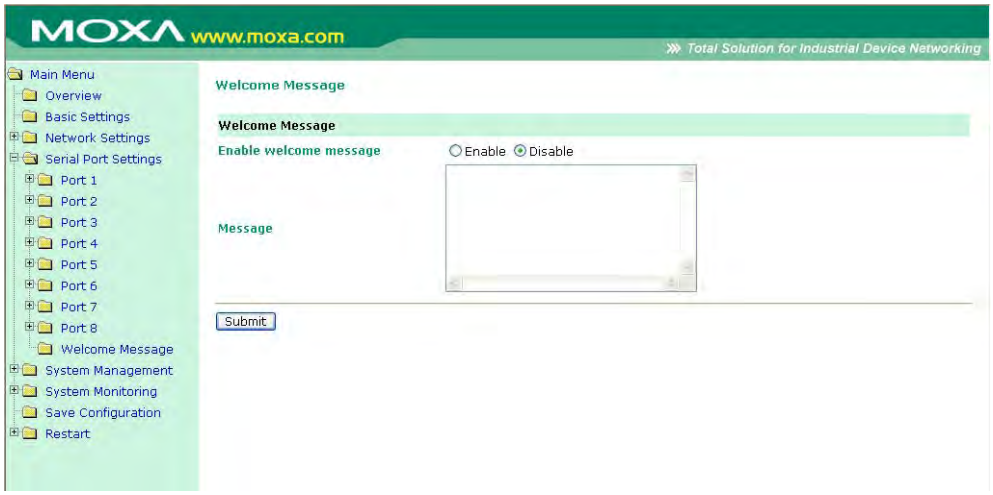
Enable modem (default=Disable)

Initial string: Use this field to configure the initial string that the modem will use to establish the connection. For example, **AT&S0=1** for auto-answer.

Dial up: Use this field to configure the modem's Dial-up AT command string.

Phone number: Use this field to configure the number that the user uses to dial out.

Welcome Message



You can enable and enter a welcome message to greet dial-in or terminal users. For ports configured for other modes, the welcome message will not apply.

8

System Management Settings

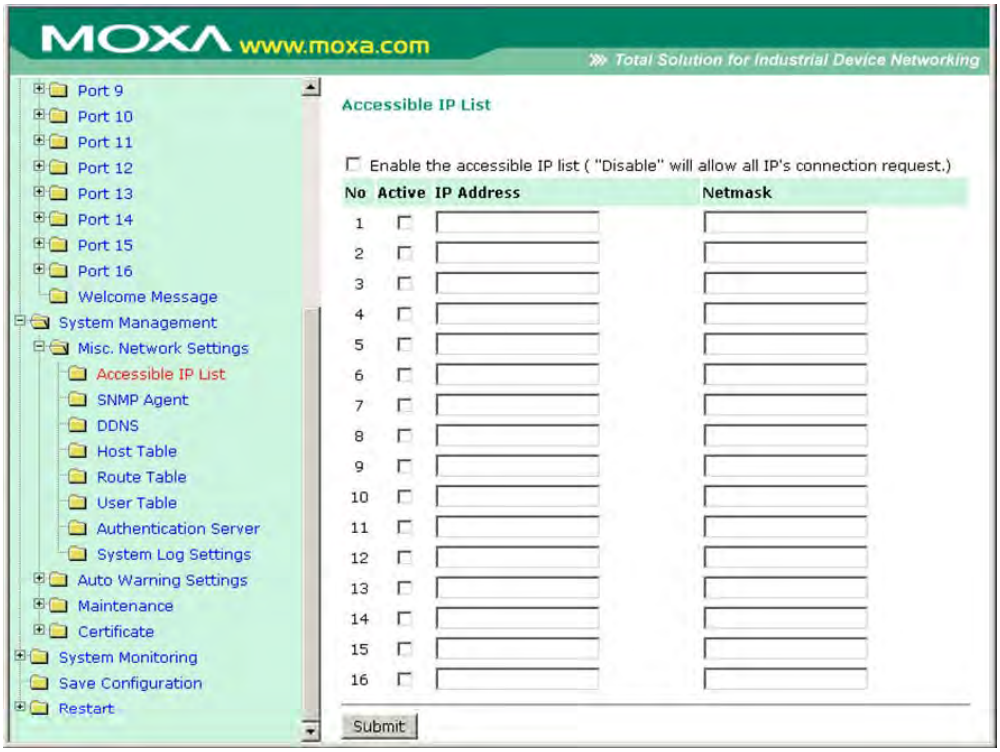
In this chapter, we describe additional server settings on the CN2600. The same configuration options are also available through the telnet and serial console.

This chapter covers the following topics:

- **Misc. Network Settings**
  - Accessible IP List
  - SNMP Agent Settings
  - DDNS
  - Host Table
  - User Table
  - Authentication Server
  - System Log Settings
- **Auto Warning Settings**
  - Event Settings
  - Serial Event Settings
  - E-mail Alert
  - SNMP Trap
- **Maintenance**
  - Console Setting
  - Ping
  - Firmware Upgrade
  - Configurating Import/Export
  - Load Factory Defaults
  - Change Password
- **Certificate**
  - Ethernet SSL Certificate Import
  - Certificate/Key Delete
- **System Monitoring**
  - Serial to Network Connections
  - Serial Port Status
  - Serial Port Error Count
  - Serial Port Settings
  - Network Connections
  - Network Statistics
  - Serial Data Log
  - System Log
  - Routing
- **Save Configuration**
- **Restart**
  - Restart System
  - Restart Ports

Misc. Network Settings

Accessible IP List



The CN2600 uses an IP address-based filtering method to control access to its serial ports.

The Accessible IP list allows you restrict network access to the CN2600. Access is controlled by IP address. When the accessible IP list is enabled, a host's IP address must be listed in order to have access to the CN2600. You may add a specific address or range of addresses by using a combination of IP address and netmask, as follows:

To allow access to a specific IP address
Enter the IP address in the corresponding field; enter **255.255.255.255** for the netmask.

To allow access to hosts on a specific subnet
For both the IP address and netmask, use **0** for the last digit (e.g., **192.168.1.0** and **255.255.255.0**).

To allow unrestricted access
Deselect the **Enable the accessible IP list** option.

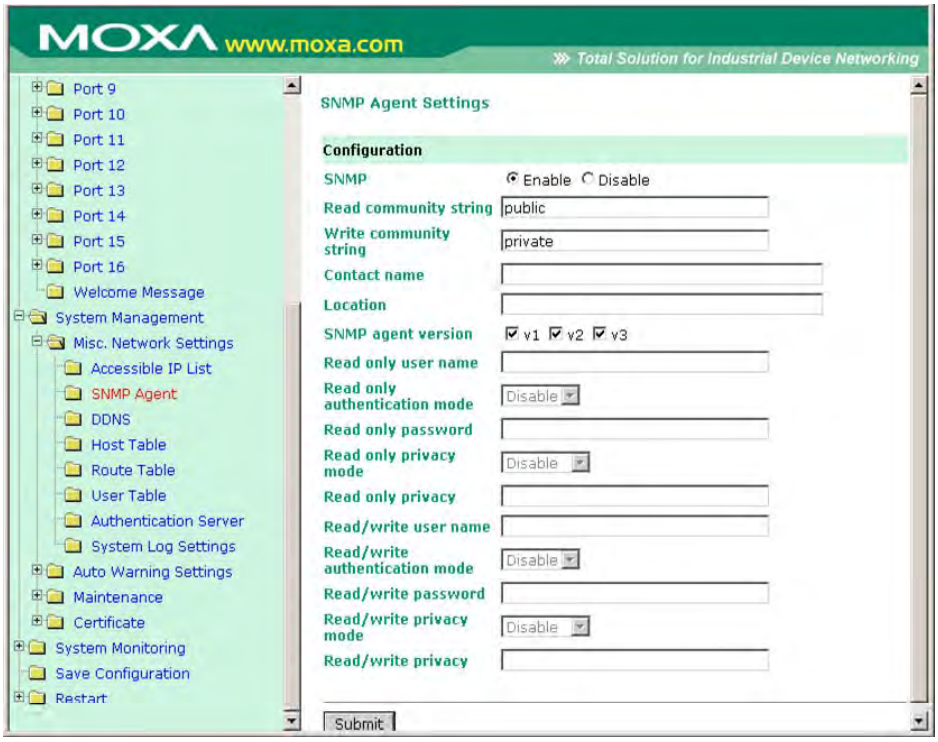
Refer to the following table for more configuration examples.

Allowed hosts	Entered IP address/Netmask
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

ATTENTION

The Accessible IP List will not be used if you configure the serial port for DRDAS Real COM mode or DRDAS TCP Server mode. In this case, the Primary IP address, three Backup IP addresses, and filtering method from the DRDAS configuration will be used.

SNMP Agent Settings



SNMP: To enable the SNMP Agent function, select the **Enable** option, and enter a community name (e.g., **public**).

Read community string (default=public): This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.

Write community string (default=private): This is a text password mechanism that is used to weakly authenticate changes to agents of managed network devices.

Contact name: The optional SNMP contact information usually includes an emergency contact name and telephone or pager number.

Location: Use this optional field to specify the location string for SNMP agents such as the CN2600. This string is usually set to the street address where the CN2600 is physically located.

SNMP agent version: The CN2600 supports SNMP V1, V2, and V3.

Read-only and Read/write access control

The following fields allow you to define user names, passwords, and authentication parameters for two levels of access: read-only and read/write. The name of the field will indicate which level of access it refers to. For example, **Read only** authentication mode allows you to configure the authentication mode for read-only access, whereas **Read/write** authentication mode allows you to configure the authentication mode for read/write access. For each level of access, you may configure the following:

User name: Use this optional field to identify the user name for the specified level of access.

Authentication mode (default=Disable): Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication

Privacy mode (default=Disable): Use this field to enable to disable DES_CBC data encryption for the specified level of access.

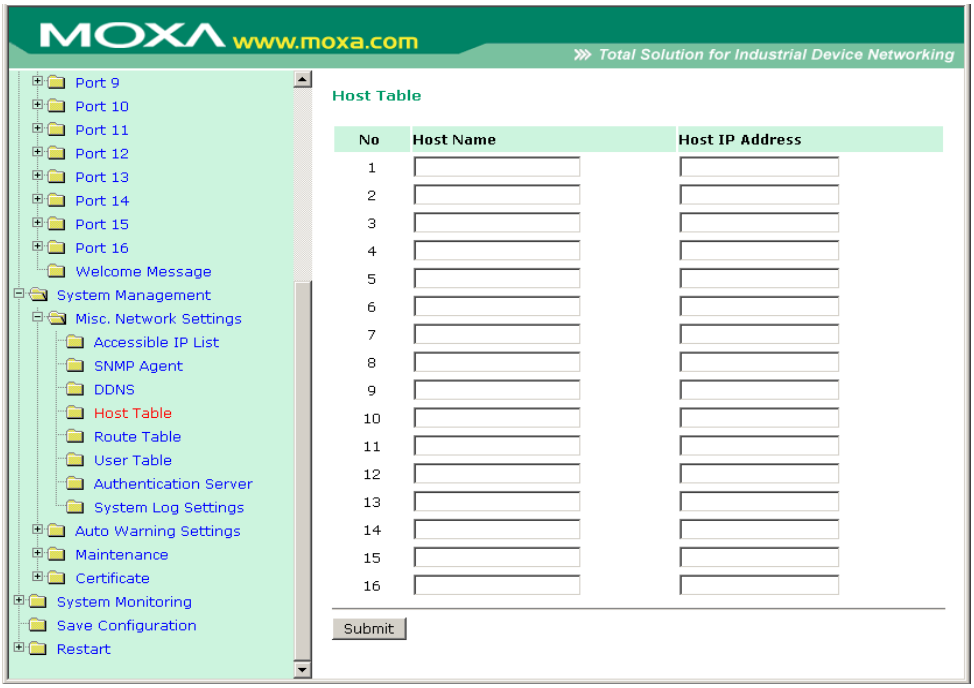
Password: Use this field to set the password for the specified level of access.

Privacy: Use this field to define the encryption key for the specified level of access

DDNS

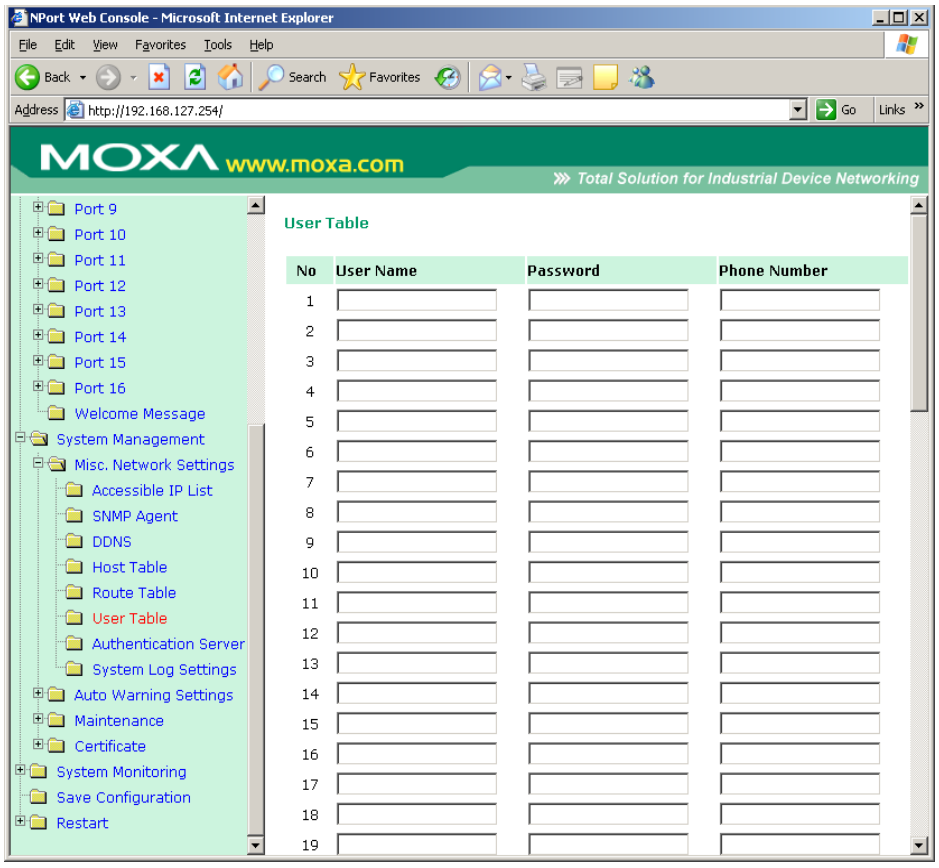
Please refer t to Appendix C, Dynamic Domain Name Server, for information on setting up DDNS on your CN2600.

Host Table



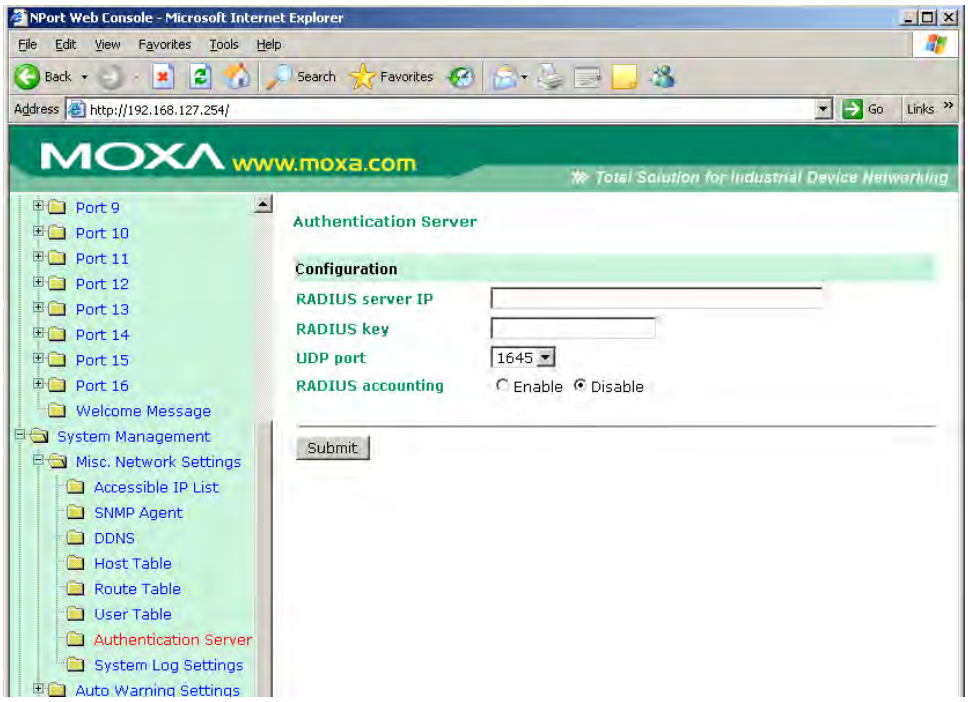
The Host Table may be used to simplify IP address entry on the CN2600 console by assigning a Host Name to a Host IP Address. When you assign a Host Name to a Host IP Address, you may then use the Host Name for some fields on the console rather than entering the IP address. Up to 16 entries can be stored on the Host Table.

User Table



The CN2600 User Table may be used for to authenticate users for terminal or reverse terminal access and is useful if you do not have an external RADIUS server for authentication. The CN2600 User Table stores up to 64 entries, with fields for User Name, Password, and Phone Number.

Authentication Server



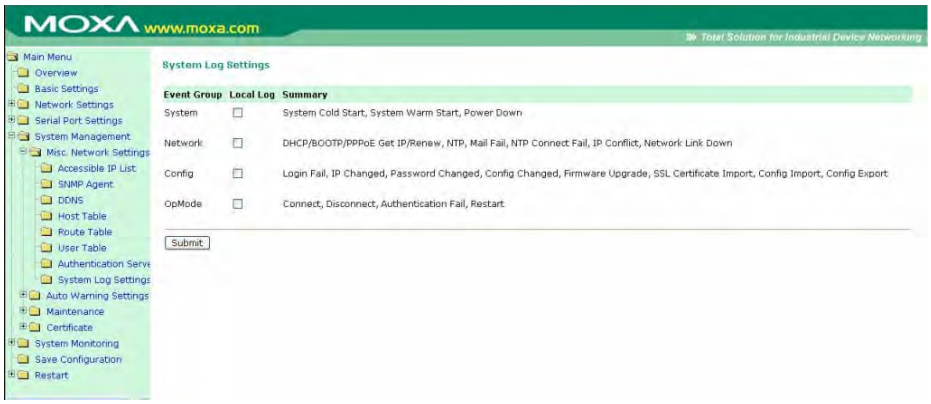
RADIUS server IP: If you are using a RADIUS server for user authentication, enter its IP address here.

RADIUS key: If you are using a RADIUS server for user authentication, enter its password here.

UDP port (default=1645): If you are using a RADIUS server, enter its UDP port assignment here.

RADIUS accounting: Use this field to enable or disable RADIUS accounting.

System Log Settings



System Log Settings allows the administrator to customize which network events are logged by the CN2600. Events are grouped into four categories, known as event groups, and the administrator selects which groups to log under Local Log. The actual system events that would be logged for each system group are listed under summary. For example, if **System** was enabled, then System Cold Start events and Power Down events (for 2AC model) would be logged.

Group	Event
System	System Cold Start, System Warm Start, Power Down
Network	DHCP/BOOTP/PPPoE Get IP/Renew, NTP, Mail Fail, NTP Connect Fail, DHCP Fail, IP Conflict, Ethernet Link Down
Config	Login Fail, IP Changed, Password Changed, Config Changed, Firmware Upgrade, SSL Key Import, Config Import, Config Export
OpMode	Connect, Disconnect, Authentication Fail, Restart

Auto Warning Settings

Event Settings

On the Event Settings page, you may configure how administrators are notified of certain system, network, and configuration events. Depending on the event, different options for automatic notification are available, as shown above. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending an SNMP Trap.

Cold start: This refers to starting the system from a power off state, or after upgrading your firmware

Warm start: This refers to restarting the CN2600 without turning the power off.

Power down: Power1 and Power2 refer to the built-in power jacks. If either power fails, the CN2600 will attempt to send an e-mail warning.

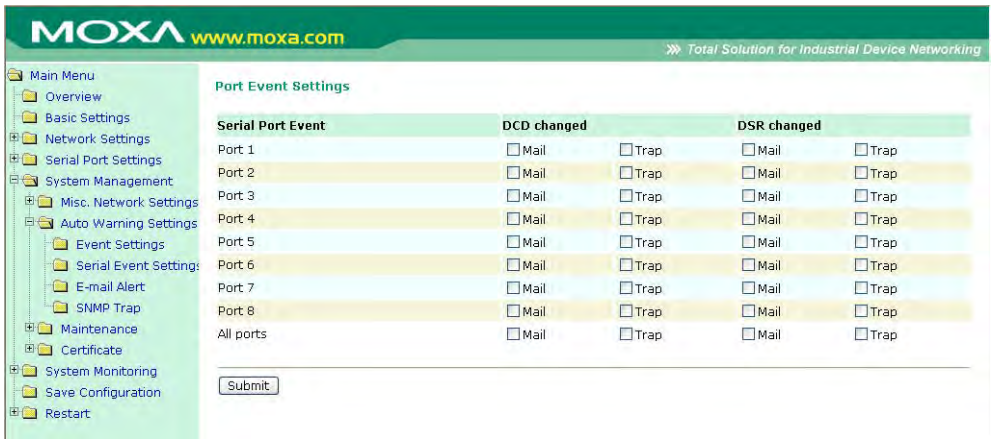
Network Event: **Ethernet1 and Ethernet2** refer to the built-in Ethernet ports. These settings configure the CN2600 to change the status of the relay output and alarm LED if the specified connection goes down.

Console(web/text) login auth fail: This field refers to a failed attempt to log in to a password-protected CN2600 console.

IP changed: With this option selected, the CN2600 will attempt to send an e-mail warning before it reboots after an IP address change. However, the CN2600 will reboot with the new IP address regardless of whether or not the e-mail transmission is successful.

Password changed: With this option selected, the CN2600 will attempt to send an e-mail warning before it reboots with a new console password. If the CN2600 is unable to send an e-mail message to the mail server within 15 seconds, it will still reboot without sending the e-mail.

Serial Event Settings



On the **Serial Event Settings** page, you may configure how administrators are notified of each serial port's DCD and DSR changes. Mail refers to sending an e-mail to a specific address. Trap refers to sending an SNMP Trap.

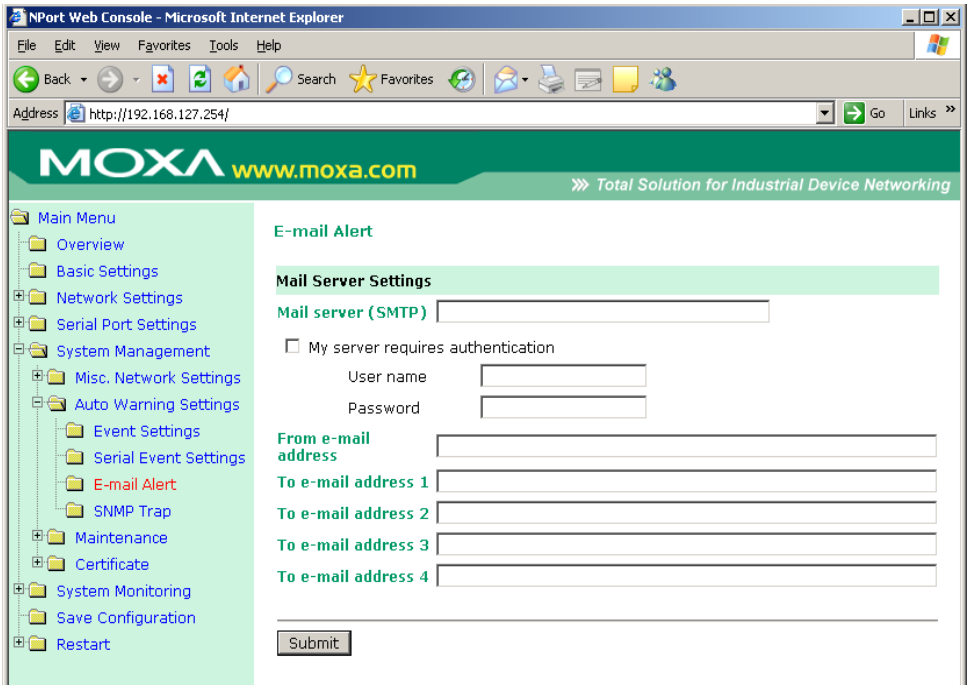
DCD changed
A change in the DCD (Data Carrier Detect) signal indicates that the modem connection status has changed. For example, if the DCD signal changes to low, it indicates that the connection line is down. When the DCD signal changes to low, the CN2600 will automatically send a warning to the administrator as configured on the Serial Event Settings page.

DSR changed
A change in the DSR (Data Set Ready) signal indicates that the data communication equipment is powered off. For example, if the DSR signal changes to low, it indicates that the data communication equipment is powered down. When the DSR signal changes to low, the CN2600 will automatically send a warning to the administrator as configured on the Serial Event Settings page.

ATTENTION

SNMP indicates a change in DCD or DSR signals but does not differentiate between the two. A change in either signal from "–" to "+" is indicated by "link up" and a change in either signal from "+" to "–" is indicated by "link down."

E-mail Alert



The E-mail Alert settings configure how e-mail warnings are sent for system and serial port events. You may configure up to 4 e-mail addresses to receive automatic warnings.

ATTENTION

Consult your Network Administrator or ISP for the proper mail server settings. The Auto warning function may not work properly if it is not configured correctly. The CN2600's SMTP AUTH supports LOGIN, PLAIN, and CRAM-MD5 (RFC 2554).

Mail server: This field is for your mail server's domain name or IP address.

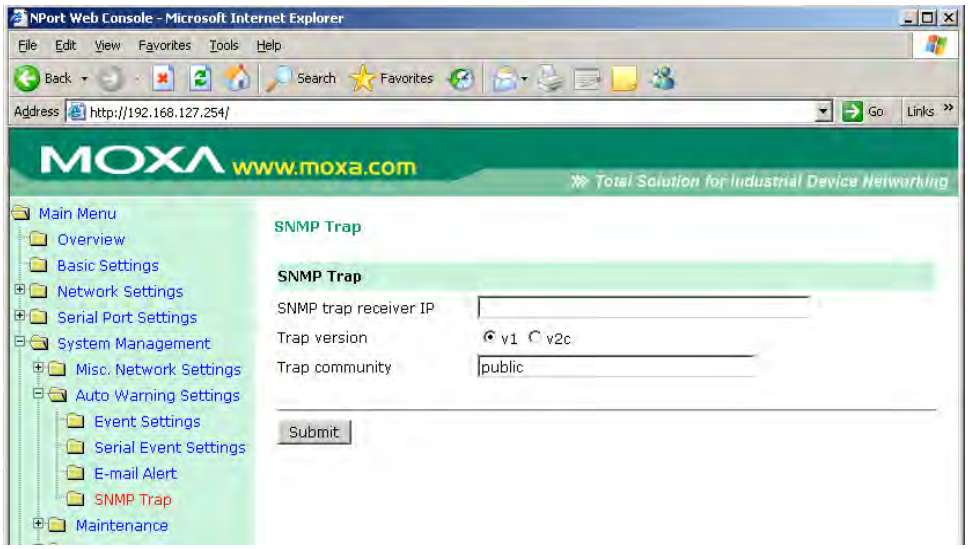
User name: This field is for your mail server's user name, if required.

Password: This field is for your mail server's password, if required.

From e-mail address: This is the e-mail address from which automatic e-mail warnings will be sent.

To e-mail address 1 to **4**: This is the e-mail address or addresses to which the automatic e-mail warnings will be sent.

SNMP Trap



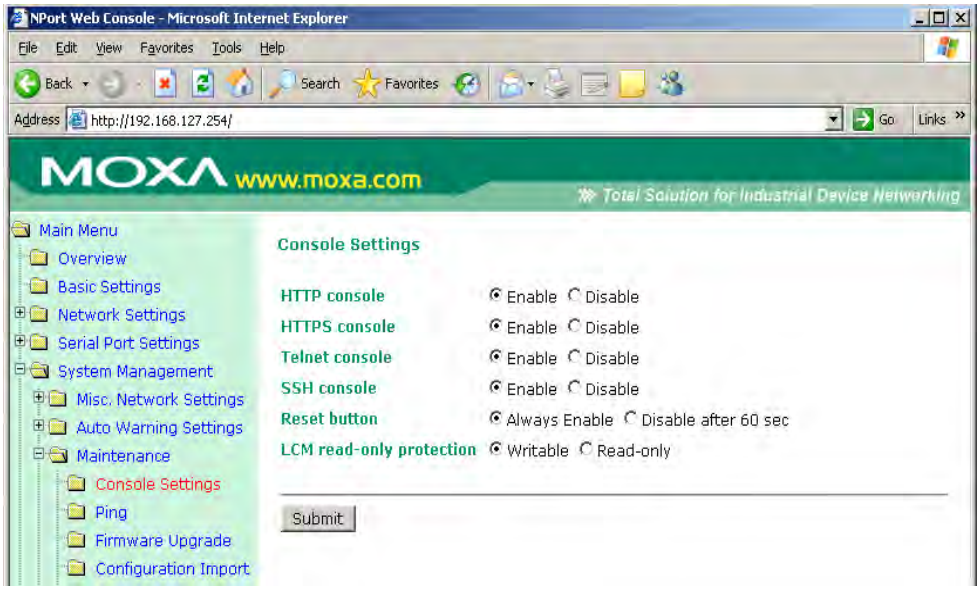
SNMP trap server IP: Use this field to indicate the IP address to use for receiving SNMP traps.

Trap version (default=v2): Use this field to select the SNMP trap version.

Trap community (default=public):Use this field to designate the SNMP trap community.

Maintenance

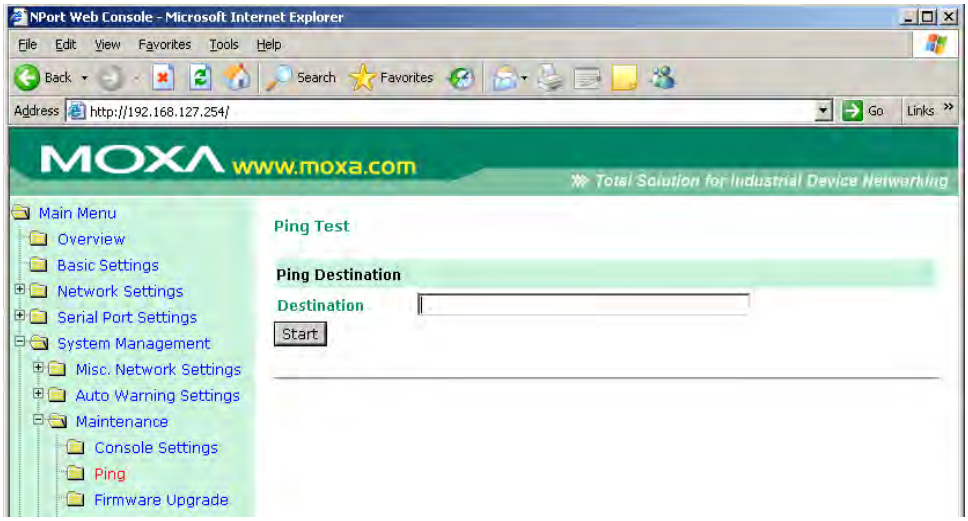
Console Setting



On this screen, access to different CN2600 configuration console options (HTTP, HTTPS, Telnet, SSH) can be enabled or disabled. The CN2600 front panel, known as the LCM (Liquid Crystal Module), may be configured for read-only or writeable access. In other words, you can use the front panel to check console settings only (read only access) or to actually make changes to the settings (writeable access). Note that if the console is password-protected and LCM is configured

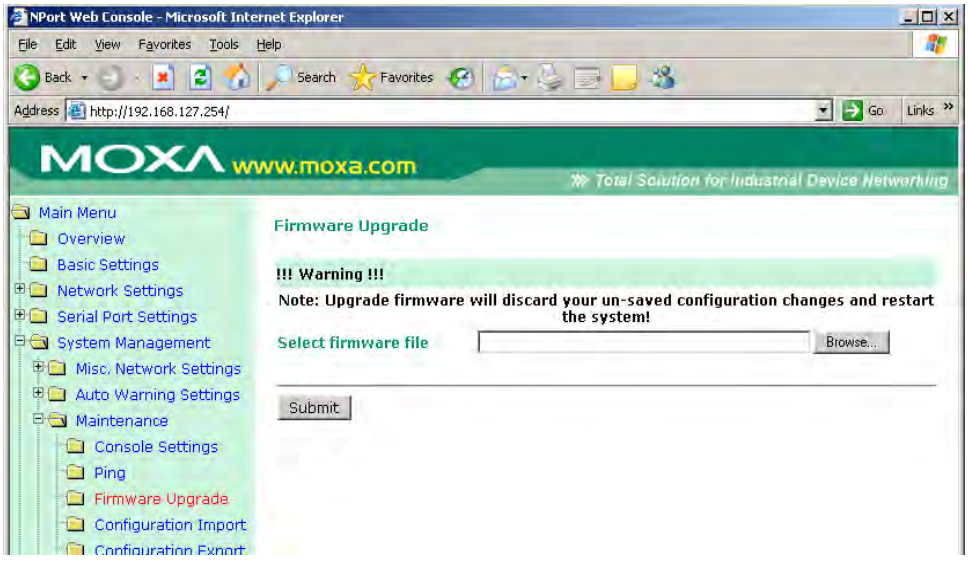
for writeable access, you will need to enter the password to submit any console setting changes. Please refer to *Change Password* later in this chapter for more information on passwords. Finally, you may also enable or disable the reset button.

Ping



You can ping an IP address from the CN2600 web console in order to test the Ethernet connection . Enter the IP address or domain name in the **Destination** field to make sure that the connection is OK.

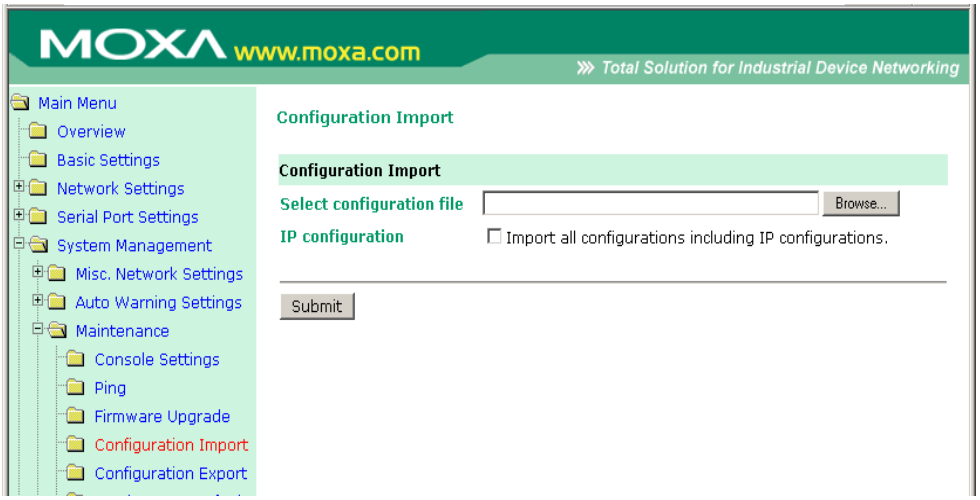
Firmware Upgrade



The CN2600's firmware can be upgraded though the web console, serial console, or through NPort Search Utility. If you have made any changes to your configuration, remember to save the configuration first before upgrading the firmware. Please refer to *Save Configuration* later in this chapter for more information. Any unsaved changes will be discarded when the firmware is upgraded. To upgrade the firmware, simply enter the file name and click **Submit**. The latest firmware can be downloaded at www.moxa.com.

Configurating Import/Export

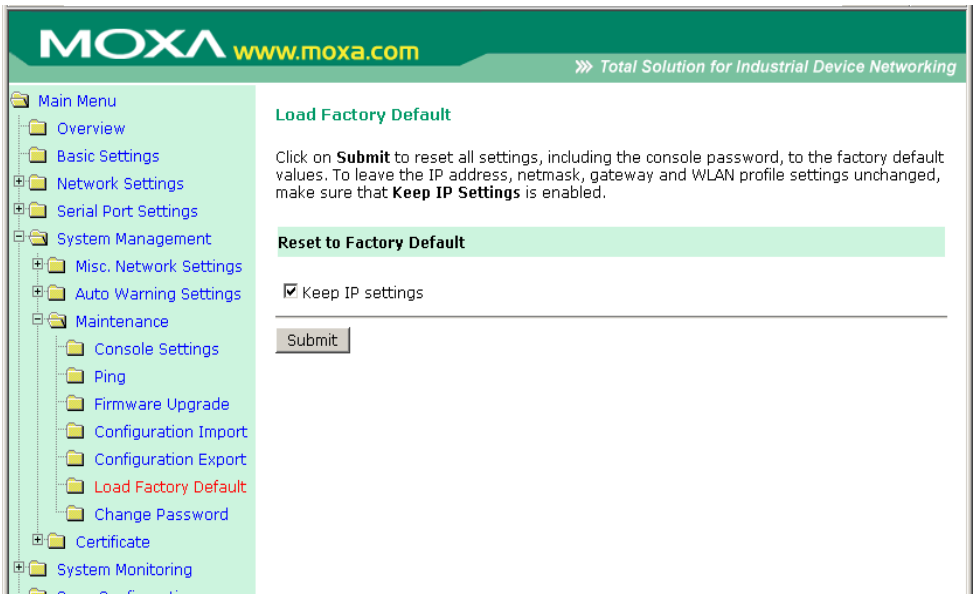
The CN2600 can share or back up its configuration by exporting all settings to a file, which can then be imported into another CN2600.



To import a configuration, go to **System Management → Maintenance → Configuration Import**. Enter the configuration file path/name and click **Submit**. The CN2600's configuration settings will be updated according to the configuration file. If you also wish to import the IP configuration (i.e., the CN2600's IP address, netmask, gateway, etc.), make sure that **Import all configurations including IP configurations** is checked off.

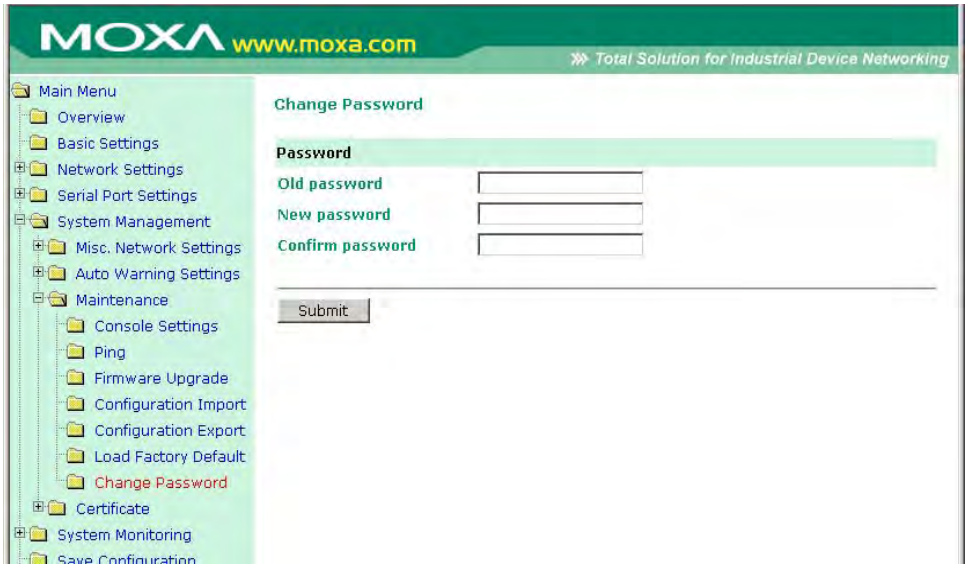
To export a configuration, go to **System Management → Maintenance → Configuration Export** and click **Download**. A standard download window will appear, and you will be able to download the configuration into a file name and location of your choice.

Load Factory Defaults



This function will reset all of CN2600's settings to the factory default values. All previous settings including the console password will be lost. If you wish to keep the CN2600 IP address, netmask, and other IP settings, make sure **Keep IP settings** is checked off before loading the factory defaults.

Change Password



For all changes to the CN2600's password protection settings, you will first need to enter the old password. Leave this blank if you are setting up password protection for the first time. To set up a new password or change the existing password, enter your desired password under both **New password** and **Confirm password**. To remove password protection, leave the **New password** and **Confirm password** boxes blank.

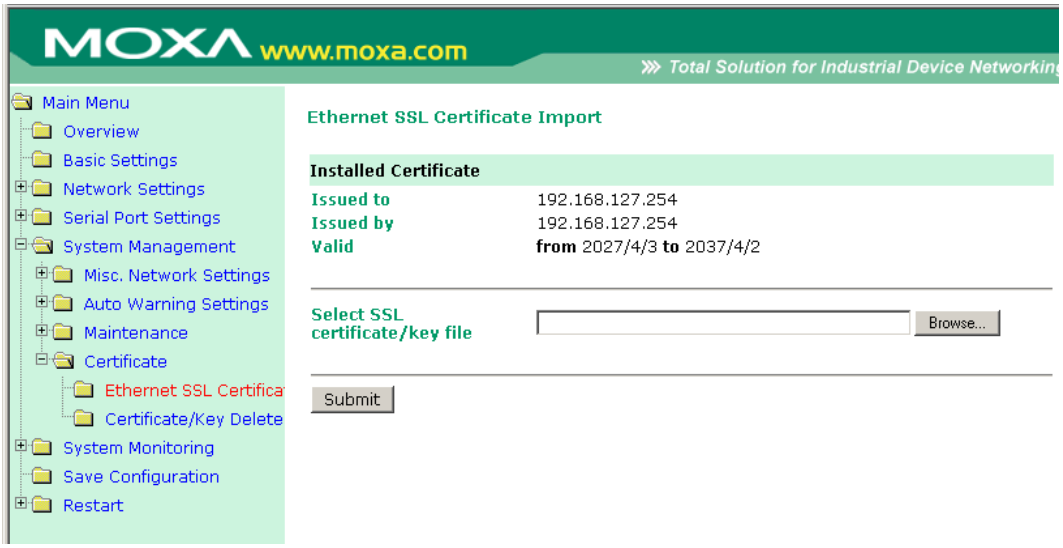
ATTENTION

If you forget the password, the ONLY way to configure the CN2600 is by using the reset button on the CN2600's casing to load the factory defaults.

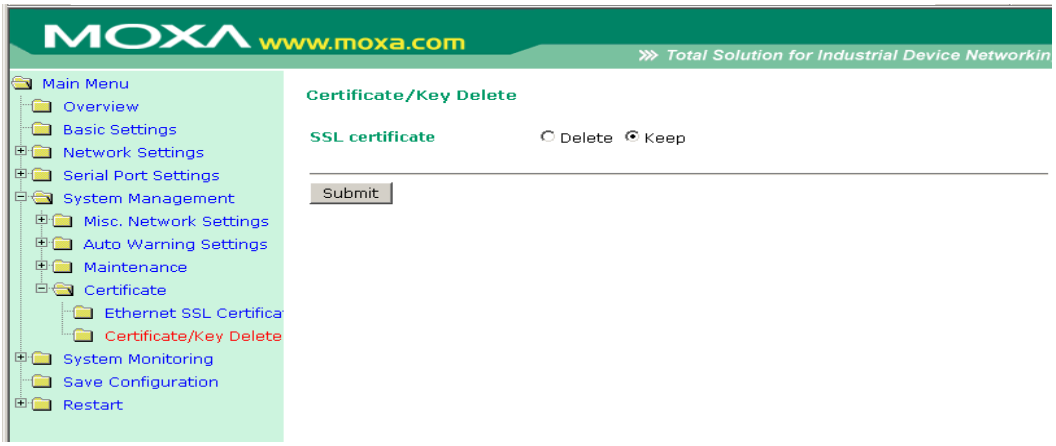
Before you set a password for the first time, it is a good idea to export the configuration to a file when you have finished setting up your CN2600. Your configuration can then be easily imported back into the CN2600 if you need to reset the CN2600 due to a forgotten password or for other reasons. Please refer to the section on *Configuration Import/Export* earlier in this chapter for more details.

Certificate

Ethernet SSL Certificate Import



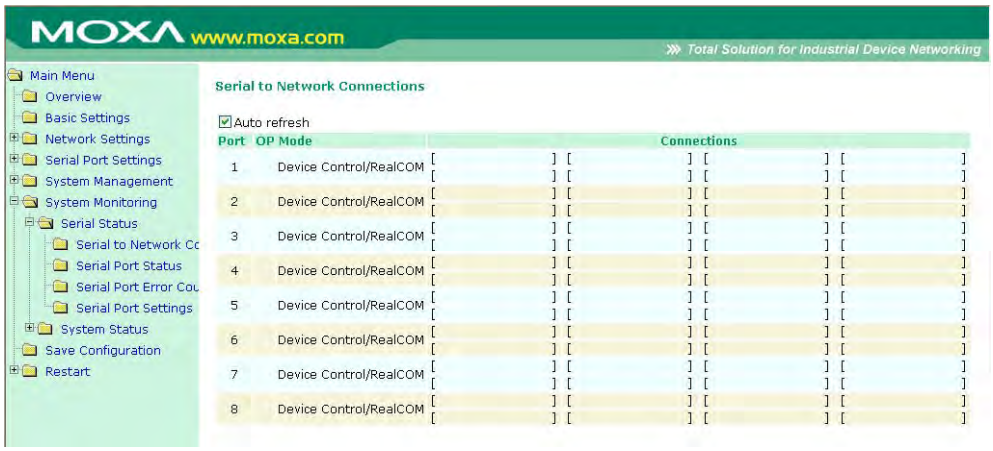
Certificate/Key Delete



System Monitoring

Serial to Network Connections

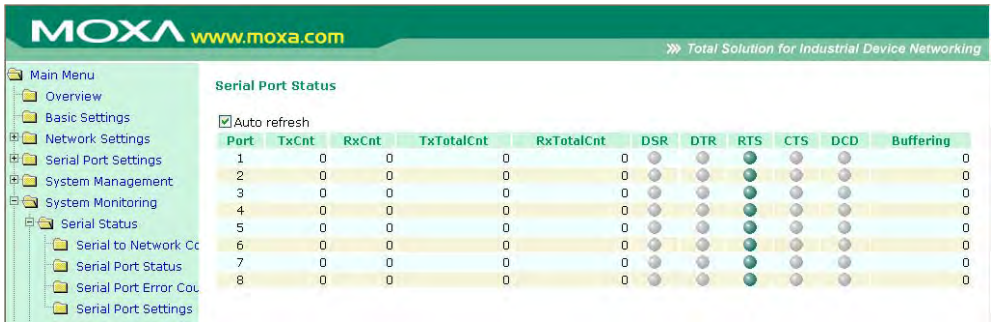
Go to **Serial to Network Connections** under **Serial Status** to view the operation mode and status of each connection, for each serial port. All monitor functions will refresh automatically every 5 seconds.



Serial Port Status

Go to **Serial Port Status** under **Serial Status** to view the current status of each serial port.

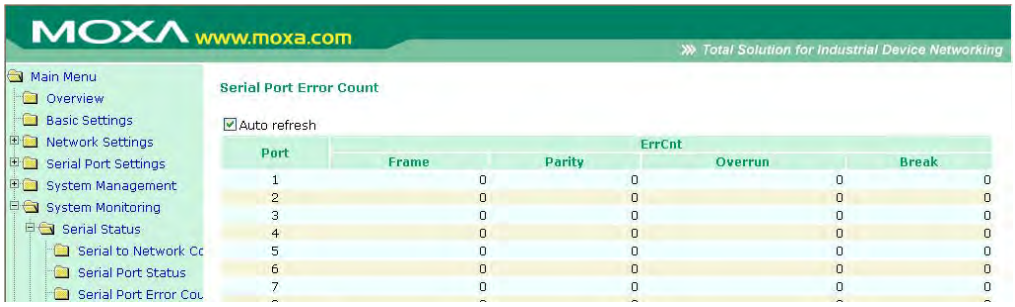
Serial Port Status → Buffering


MOXA www.moxa.com
Total Solution for Industrial Device Networking
Main Menu
Overview
Basic Settings
Network Settings
Serial Port Settings
System Management
System Monitoring
Serial Status
Serial to Network Cc
Serial Port Status
Serial Port Error Cou
Serial Port Settings
Serial Port Status
Auto refresh
Port TxCnt RxCnt TxTotalCnt RxTotalCnt DSR DTR RTS CTS DCD Buffering
1 0 0 0 0 0
2 0 0 0 0 0
3 0 0 0 0 0
4 0 0 0 0 0
5 0 0 0 0 0
6 0 0 0 0 0
7 0 0 0 0 0
8 0 0 0 0 0

Monitor port buffering usage (bytes) of each serial port.

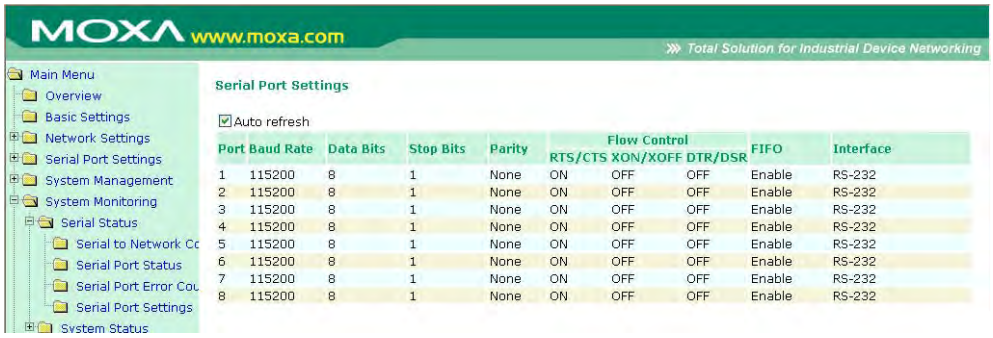
Serial Port Error Count

Go to **Serial Port Error Count** under **Serial Status** to view the error count for each serial port.



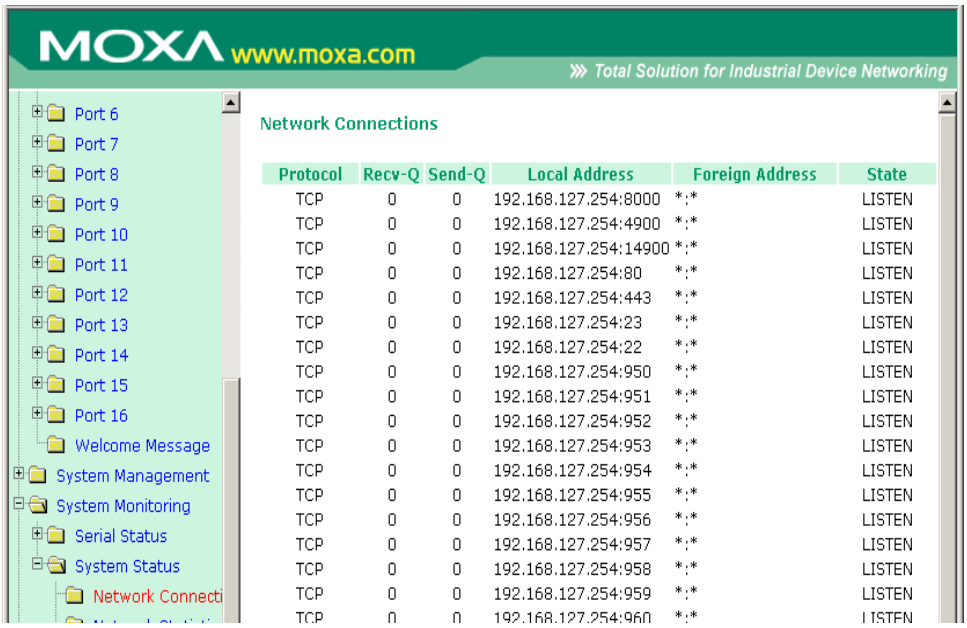
Serial Port Settings

Go to **Serial Port Settings** under **Serial Status** to view a summary of the settings for each serial port.


MOXA www.moxa.com
Total Solution for Industrial Device Networking
Main Menu
Overview
Basic Settings
Network Settings
Serial Port Settings
System Management
System Monitoring
Serial Status
Serial to Network Cc
Serial Port Status
Serial Port Error Cou
Serial Port Settings
System Status
Serial Port Settings
Auto refresh
Port Baud Rate Data Bits Stop Bits Parity Flow Control RTS/CTS XON/XOFF DTR/DSR FIFO Interface
1 115200 8 1 None ON OFF OFF Enable RS-232
2 115200 8 1 None ON OFF OFF Enable RS-232
3 115200 8 1 None ON OFF OFF Enable RS-232
4 115200 8 1 None ON OFF OFF Enable RS-232
5 115200 8 1 None ON OFF OFF Enable RS-232
6 115200 8 1 None ON OFF OFF Enable RS-232
7 115200 8 1 None ON OFF OFF Enable RS-232
8 115200 8 1 None ON OFF OFF Enable RS-232

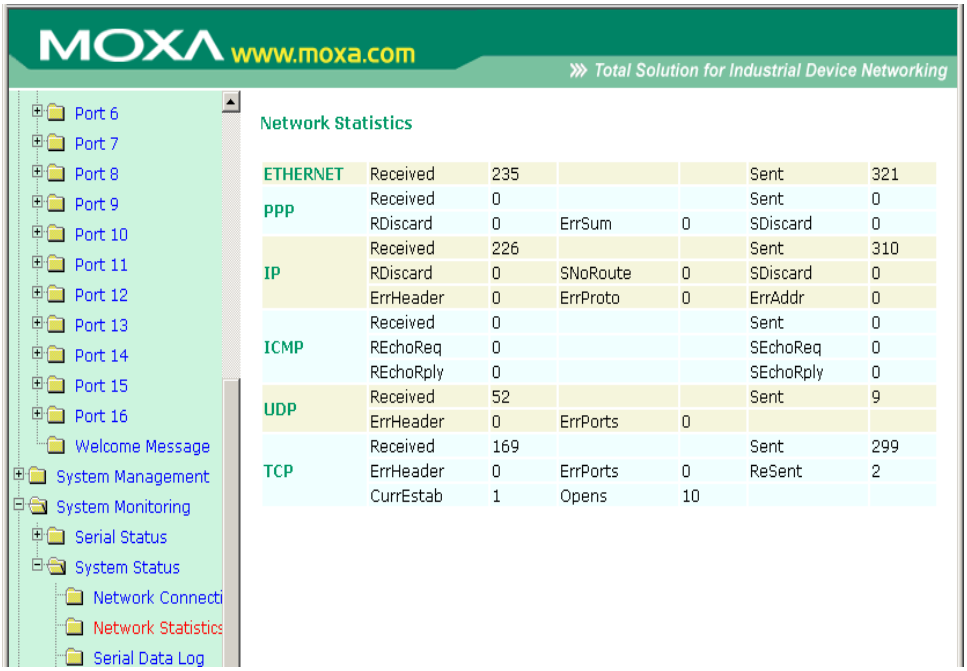
Network Connections

Go to **Network Connections** under **System Status** to view network connection information.


MOXA www.moxa.com
Total Solution for Industrial Device Networking
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Welcome Message
System Management
System Monitoring
Serial Status
System Status
Network Connecti
Network Connections
Protocol Recv-Q Send-Q Local Address Foreign Address State
TCP 0 0 192.168.127.254:8000 *:* LISTEN
TCP 0 0 192.168.127.254:4900 *:* LISTEN
TCP 0 0 192.168.127.254:14900 *:* LISTEN
TCP 0 0 192.168.127.254:80 *:* LISTEN
TCP 0 0 192.168.127.254:443 *:* LISTEN
TCP 0 0 192.168.127.254:23 *:* LISTEN
TCP 0 0 192.168.127.254:22 *:* LISTEN
TCP 0 0 192.168.127.254:950 *:* LISTEN
TCP 0 0 192.168.127.254:951 *:* LISTEN
TCP 0 0 192.168.127.254:952 *:* LISTEN
TCP 0 0 192.168.127.254:953 *:* LISTEN
TCP 0 0 192.168.127.254:954 *:* LISTEN
TCP 0 0 192.168.127.254:955 *:* LISTEN
TCP 0 0 192.168.127.254:956 *:* LISTEN
TCP 0 0 192.168.127.254:957 *:* LISTEN
TCP 0 0 192.168.127.254:958 *:* LISTEN
TCP 0 0 192.168.127.254:959 *:* LISTEN

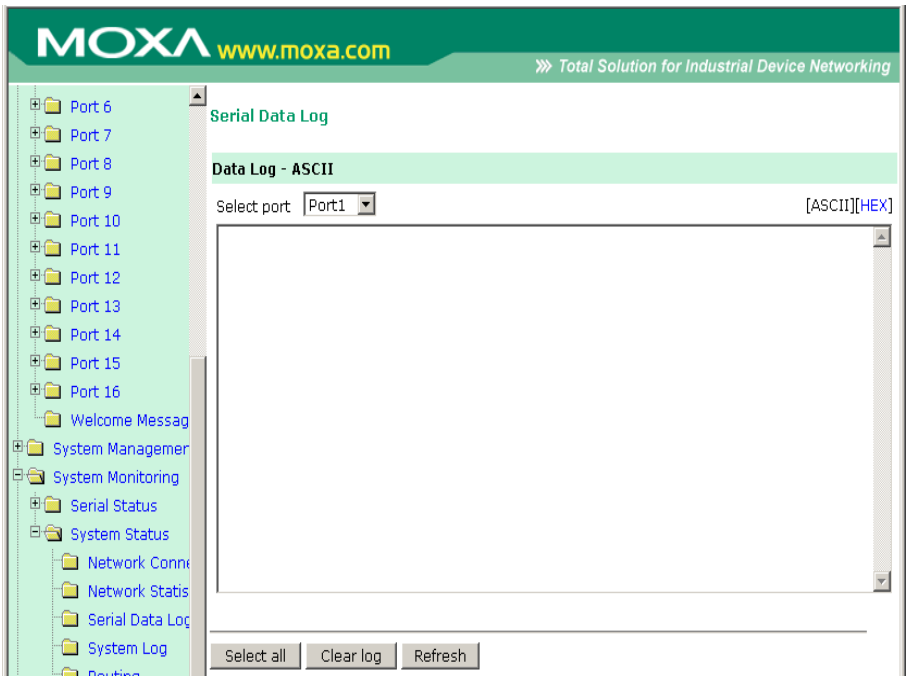
Network Statistics

Go to **Network Statistics** under **System Status** to view network statistics.



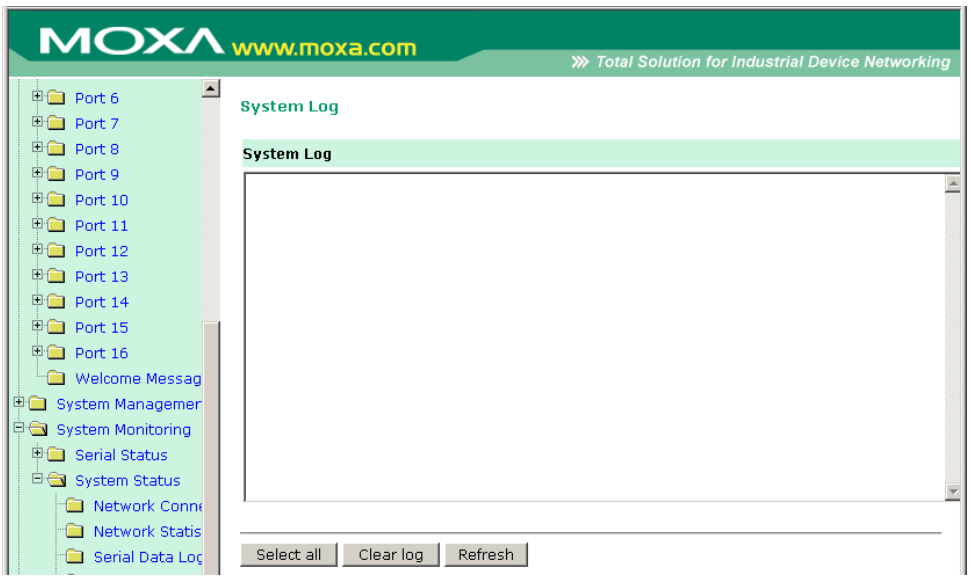
Serial Data Log

Data logs for each serial port can be viewed in ASCII or HEX format. After selecting the serial port and format, you may click **Select all** to select the entire log if you wish to copy and paste the contents into a text file.



System Log

This option displays the system log. You may click **Select all** to select the entire log if you wish to copy and paste the contents into a text file.

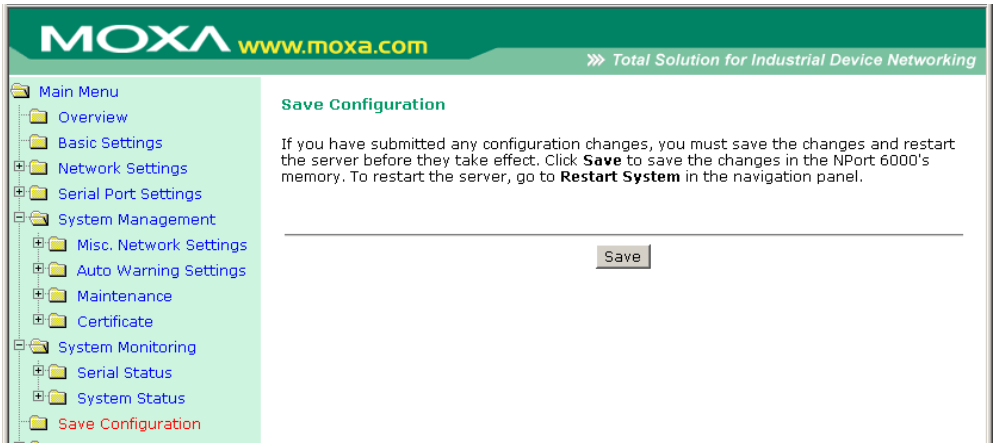


Routing

Go to **Routing** under **System Status** to display the routing information.

Save Configuration

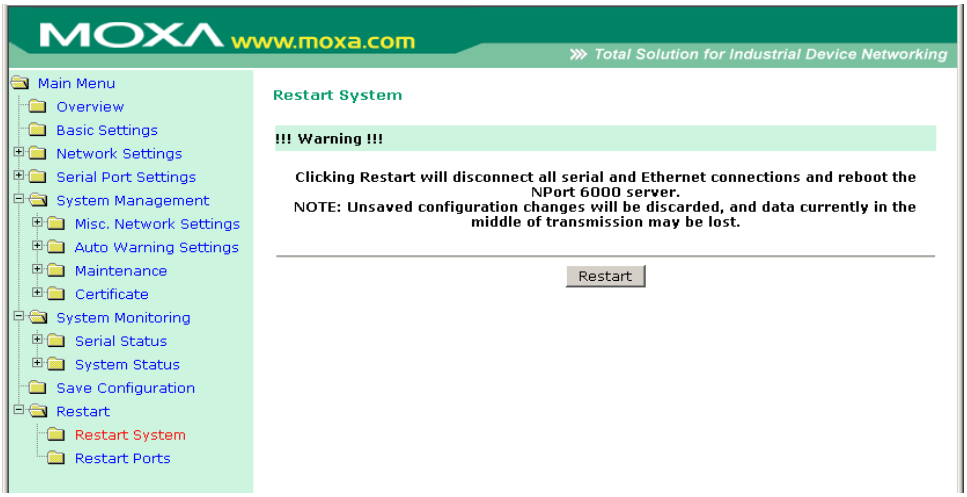
Go to **Save Configuration** and then click **Save** to save the your submitted configuration changes to the CN2600's flash memory. The configuration changes will then be effective when the CN2600 is restarted. If you do not save your changes before restarting, they will be discarded.


MOXA www.moxa.com
Total Solution for Industrial Device Networking
Main Menu
Overview
Basic Settings
Network Settings
Serial Port Settings
System Management
Misc. Network Settings
Auto Warning Settings
Maintenance
Certificate
System Monitoring
Serial Status
System Status
Save Configuration
Save Configuration
If you have submitted any configuration changes, you must save the changes and restart the server before they take effect. Click Save to save the changes in the NPort 6000's memory. To restart the server, go to Restart System in the navigation panel.
Save

Restart

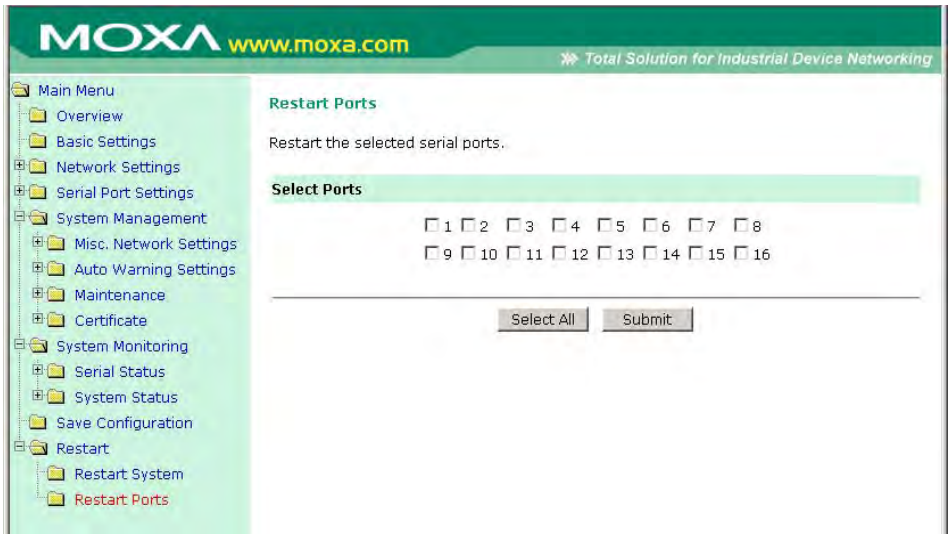
Restart System

Go to **Restart System** under **Restart** and then click **Restart** to restart the CN2600. Ensure that you save all your configuration changes before you restart the system or else these changes will be lost.



Restart Ports

Go to **Restart Ports** under **Restart** and then select the ports to be restarted. Click **Select All** to select all the ports. Click **Submit** to restart the selected ports.



9

Software Installation/Configuration

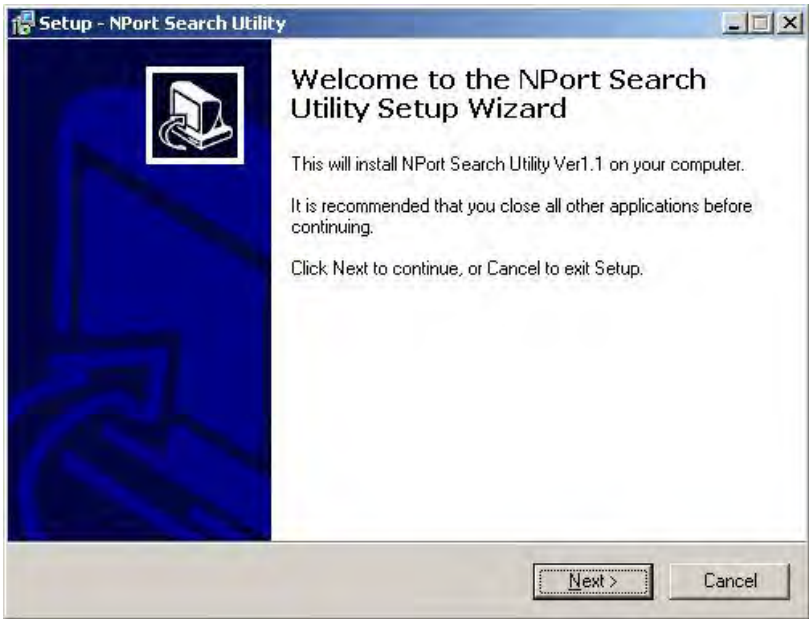
The following topics are covered in this chapter:

- **NPort Search Utility**
  - Installing NPort Search Utility
  - Configuring NPort Search Utility
- **Windows Driver Manager**
  - Installing NPort Windows Driver Manager
  - Using NPort Windows Driver Manager
- **Windows Monitor Utility**
  - Installing the NPort Monitor Utility
  - Using the NPort Monitor Utility
- **Linux Real TTY Drivers**
  - Basic Procedures
  - Hardware Setup
  - Installing Linux Real TTY Driver Files
  - Mapping TTY Ports
  - Removing Mapped TTY Ports
  - Removing Linux Driver Files
- **The UNIX Fixed TTY Driver**
  - Installing the UNIX Driver
  - Configuring the UNIX Driver

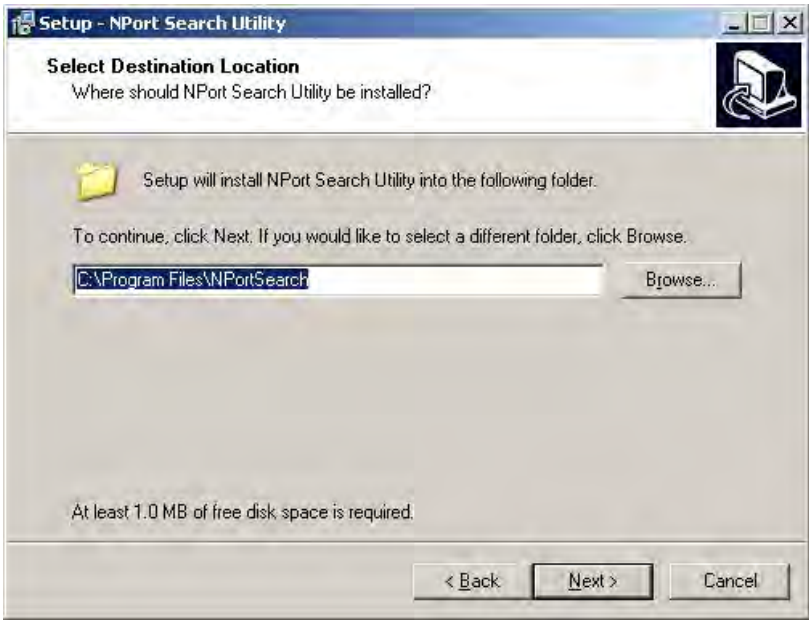
NPort Search Utility

Installing NPort Search Utility

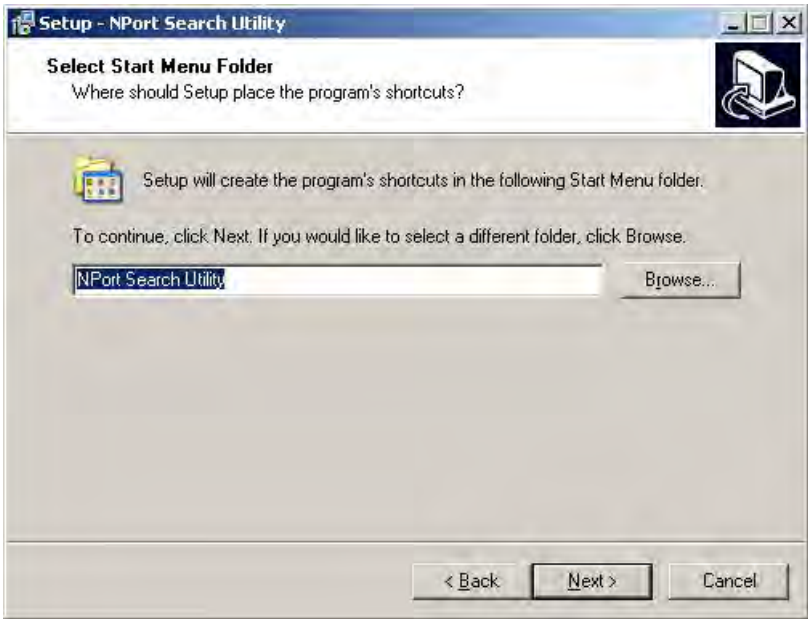
1. Click the INSTALL UTILITY button in the Installation CD auto-run window to install NPort Search Utility. Once the program starts running, click **Yes** to proceed.
2. Click **Next** when the Welcome screen opens, to proceed with the installation.


Setup - NPort Search Utility
Welcome to the NPort Search Utility Setup Wizard
This will install NPort Search Utility Ver1.1 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

3. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.


Setup - NPort Search Utility
Select Destination Location
Where should NPort Search Utility be installed?
Setup will install NPort Search Utility into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\NPortSearch
Browse...
At least 1.0 MB of free disk space is required.
< Back
Next >
Cancel

4. Click **Next** to install the program's shortcuts in the appropriate **Start Menu** folder.

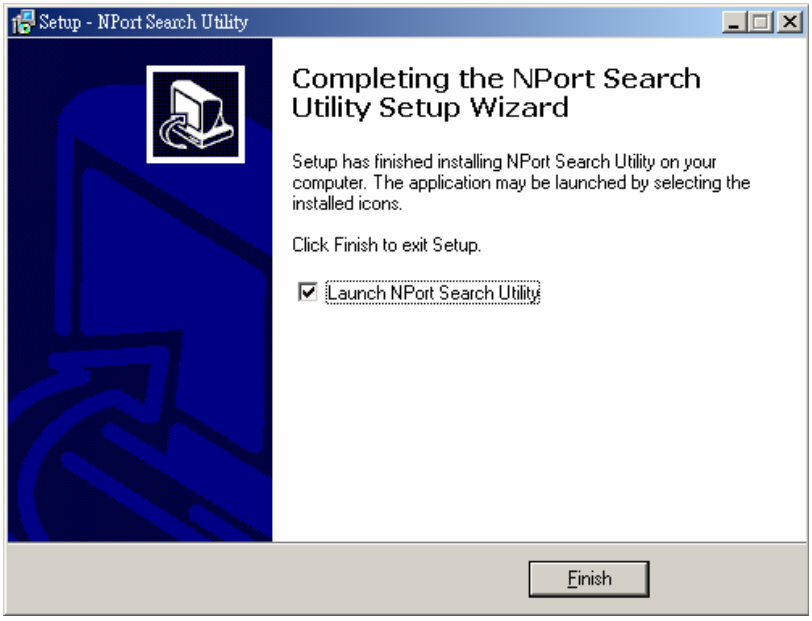

Setup - NPort Search Utility
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
NPort Search Utility
Browse...
< Back
Next >
Cancel

5. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.

Setup - NPort Search Utility
Ready to Install
Setup is now ready to begin installing NPort Search Utility on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\NPortSearch
Start Menu folder:
NPort Search Utility
< Back
Install
Cancel

6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.

7. Click **Finish** to complete the installation of Terminal Server Search Utility.

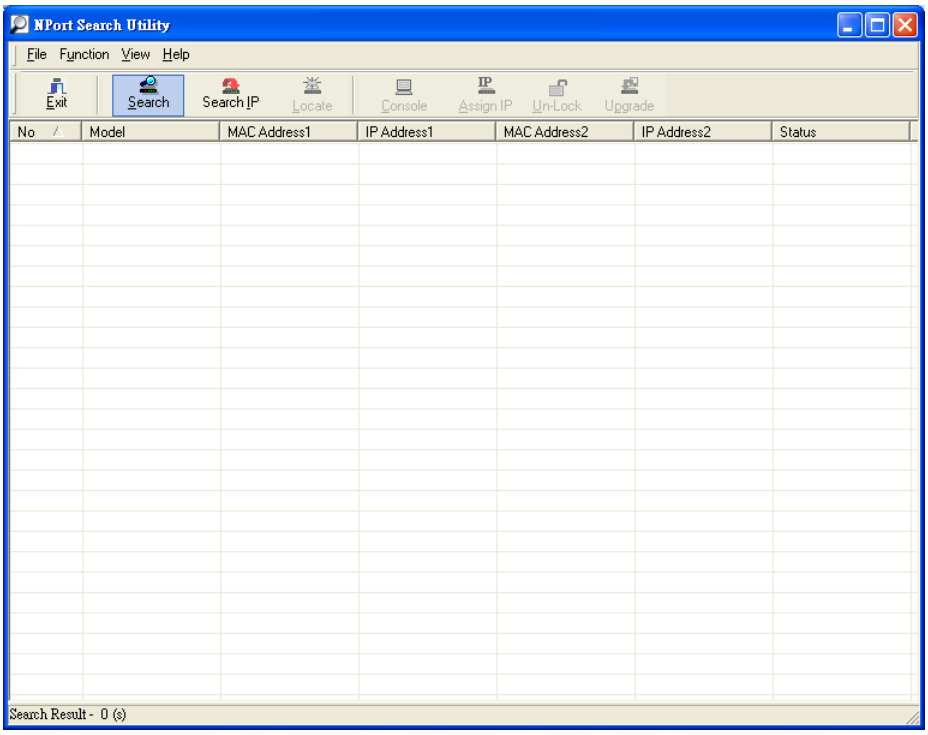

Setup - NPort Search Utility
Completing the NPort Search Utility Setup Wizard
Setup has finished installing NPort Search Utility on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch NPort Search Utility
Finish

Configuring NPort Search Utility

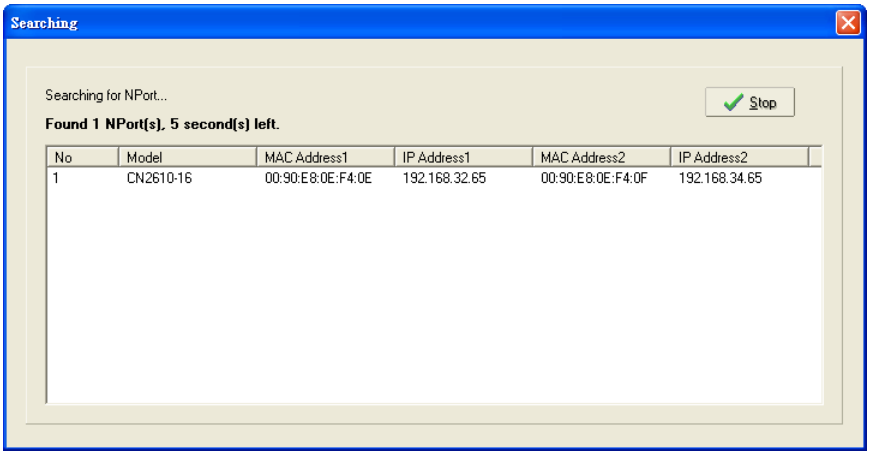
The **Broadcast Search** function is used to locate all CN2600 servers that are connected to the same LAN as your computer. After locating a CN2600, you will be able to change its IP address.

Since the **Broadcast Search** function searches by MAC address and not IP address, all CN2600 servers connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

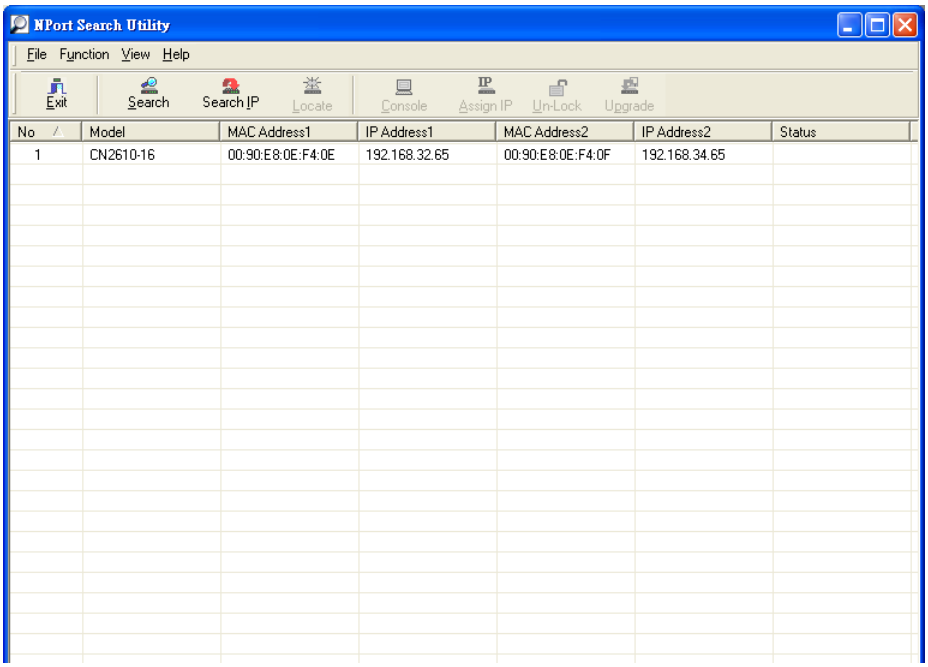
1. Open NPort Search Utility and then click the **Search** icon.



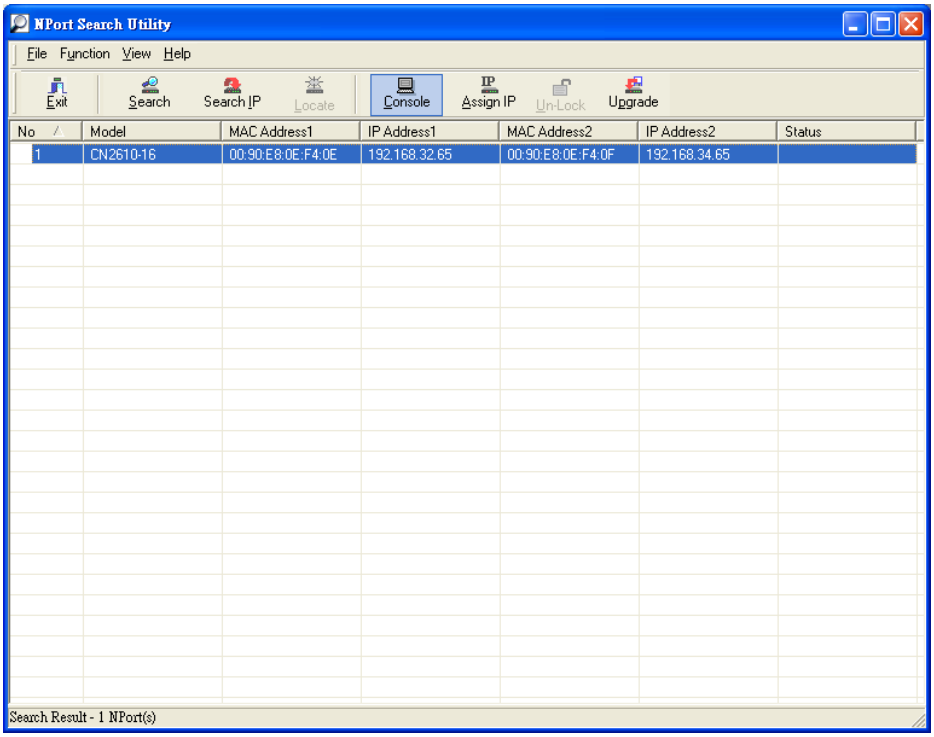
The Searching window indicates the progress of the search.



2. When the search is complete, all CN2600 servers that were located will be displayed in the NPort Search Utility window.


NPort Search Utility
File Function View Help
Exit Search Search IP Locate Console Assign IP Un-Lock Upgrade
No / Model MAC Address1 IP Address1 MAC Address2 IP Address2 Status
1 CN2610-16 00:90:E8:0E:F4:0E 192.168.32.65 00:90:E8:0E:F4:0F 192.168.34.65

To modify the configuration of the highlighted CN2600, click on the **Console** icon to open the web console. This will take you to the web console, where you can make all configuration changes. Please refer to Chapter 5, "Configuration with the Web Console," for information on how to use the web console.


NPort Search Utility
File Function View Help
Exit Search Search IP Locate Console Assign IP Un-Lock Upgrade
No / Model MAC Address1 IP Address1 MAC Address2 IP Address2 Status
1 CN2610-16 00:90:E8:0E:F4:0E 192.168.32.65 00:90:E8:0E:F4:0F 192.168.34.65
Search Result - 1 NPort(s)

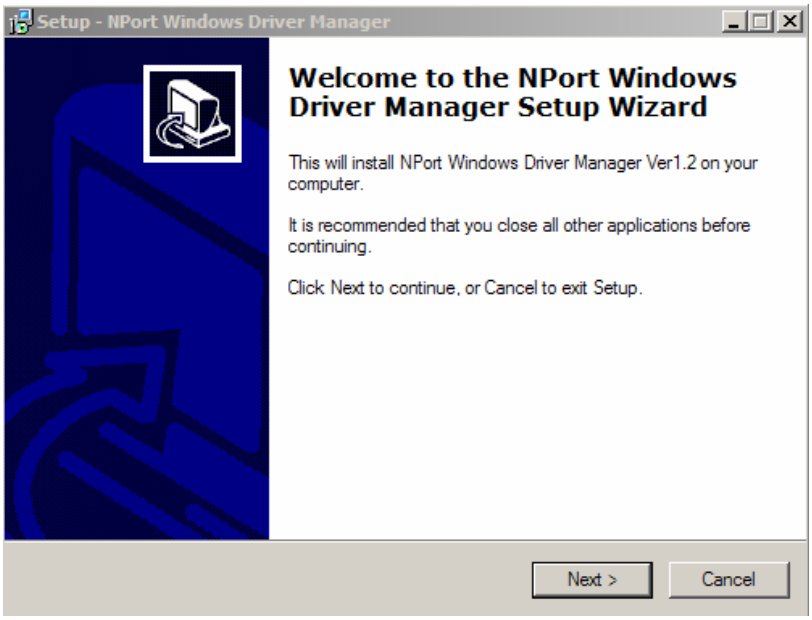
Windows Driver Manager

Installing NPort Windows Driver Manager

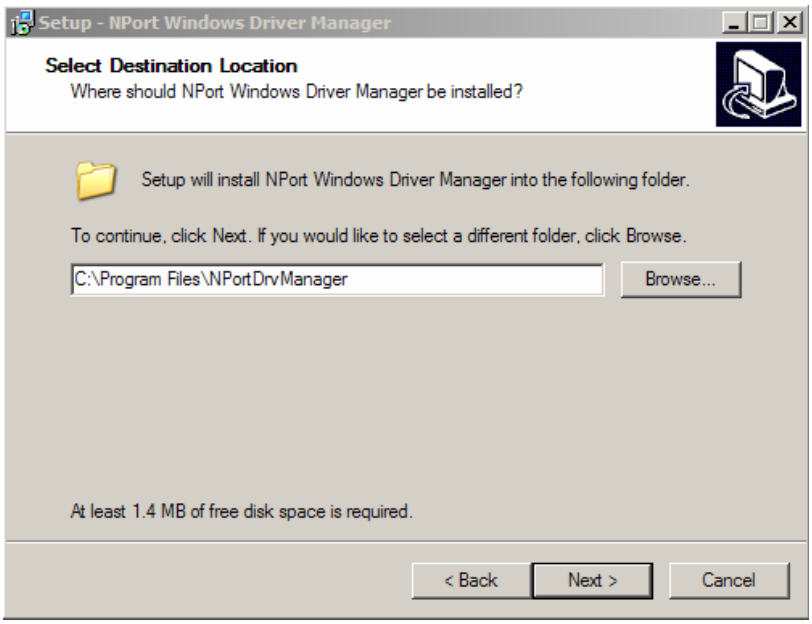
The NPort Windows Driver Manager can be used with CN2600 serial ports that are set to Real COM mode. The Driver Manager manages the installation of drivers, which allow you to map unused COM ports on your PC to serial ports on the CN2600. These drivers are designed for use with Windows 95/98/ME/NT/2000/XP/2003/Vista. When the drivers are installed and configured, devices that are attached to serial ports on the CN2600 will be treated as if they were attached to your PC's own COM ports.

If you are using the older version named Async Server Windows 2000/XP/2003 driver, please refer to Chapter 9, "Setting up Hosts" for installation information. Note that you may also download the latest Windows Driver Manager from Moxa's website.

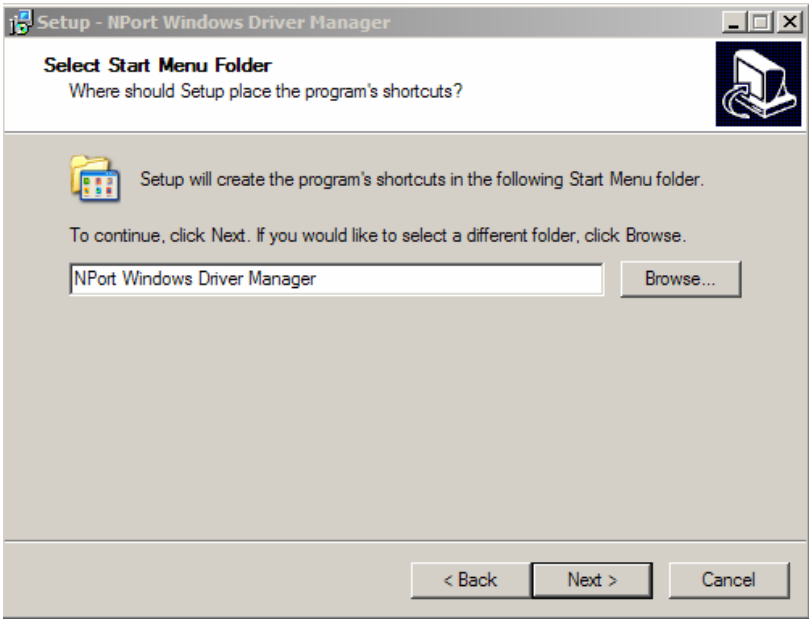
1. Click the INSTALL COM Driver button in the CN2600 Installation CD auto-run window to install NPort Windows Driver Manager. Once the installation program starts running, click **Yes** to proceed.
2. Click **Next** when the Welcome screen opens to proceed with the installation.


Setup - NPort Windows Driver Manager
Welcome to the NPort Windows Driver Manager Setup Wizard
This will install NPort Windows Driver Manager Ver1.2 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

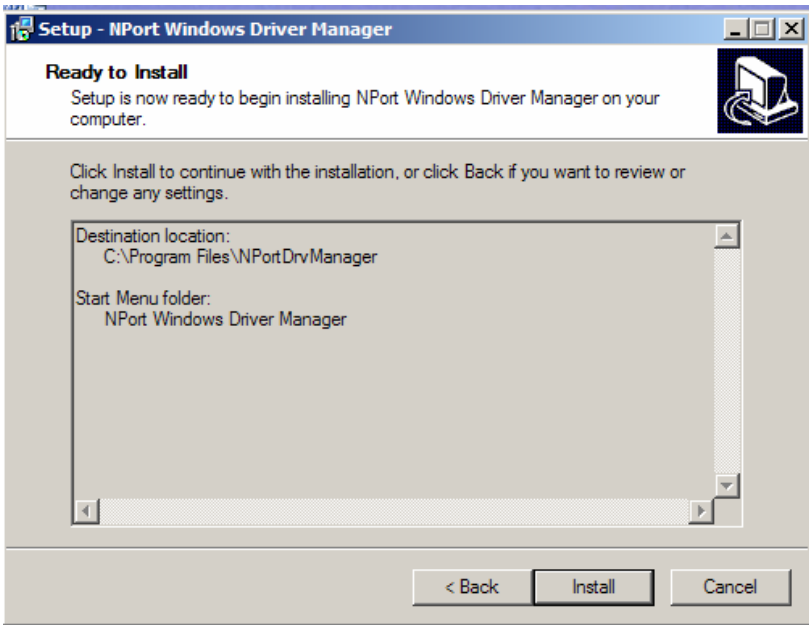
3. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.


Setup - NPort Windows Driver Manager
Select Destination Location
Where should NPort Windows Driver Manager be installed?
Setup will install NPort Windows Driver Manager into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\NPortDrvManager
Browse...
At least 1.4 MB of free disk space is required.
< Back
Next >
Cancel

4. Click **Next** to install the program's shortcuts in the appropriate **Start Menu** folder.

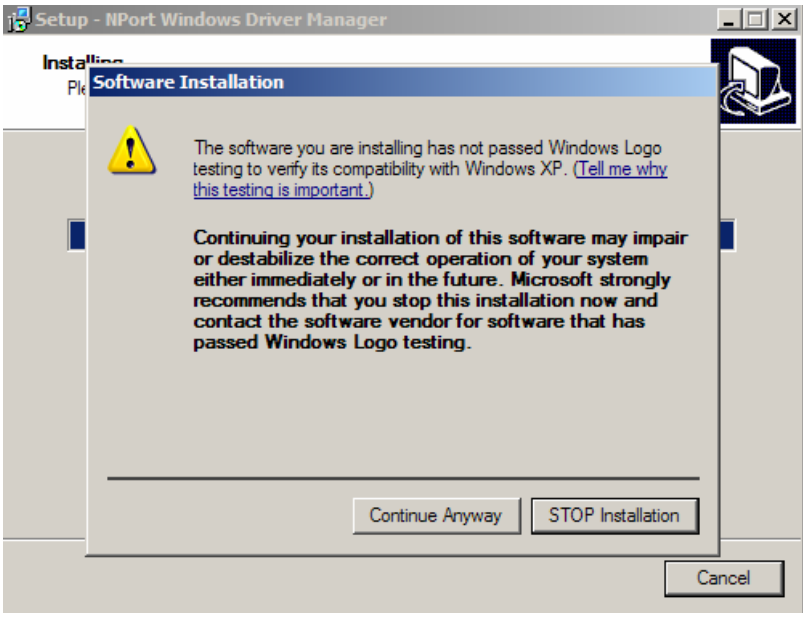

Setup - NPort Windows Driver Manager
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
NPort Windows Driver Manager
Browse...
< Back
Next >
Cancel

5. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.

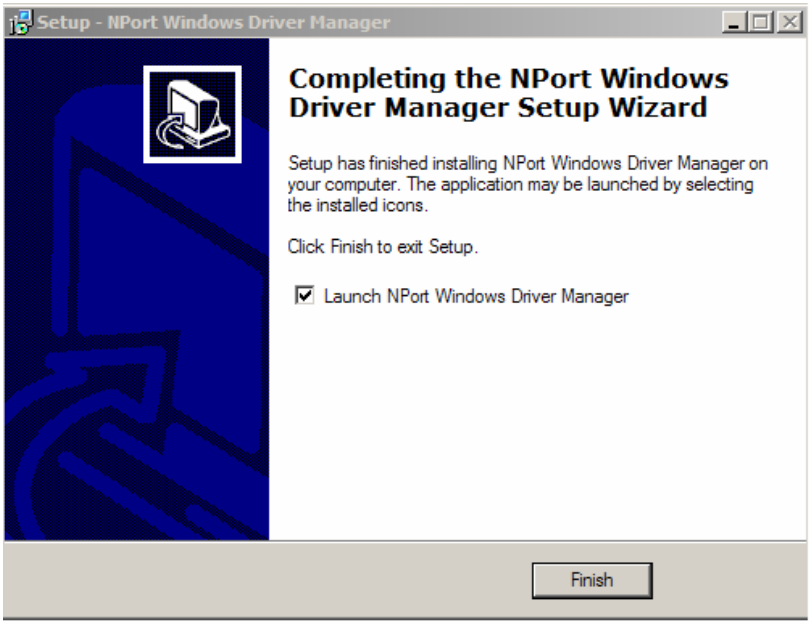

Setup - NPort Windows Driver Manager
Ready to Install
Setup is now ready to begin installing NPort Windows Driver Manager on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\NPortDrvManager
Start Menu folder:
NPort Windows Driver Manager
< Back
Install
Cancel

6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.

   In Windows XP, a message will appear indicating that the software has not passed Windows Logo testing. Click **Continue Anyway** to finish the installation.


Setup - NPort Windows Driver Manager
Software Installation
The software you are installing has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the software vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation
Cancel

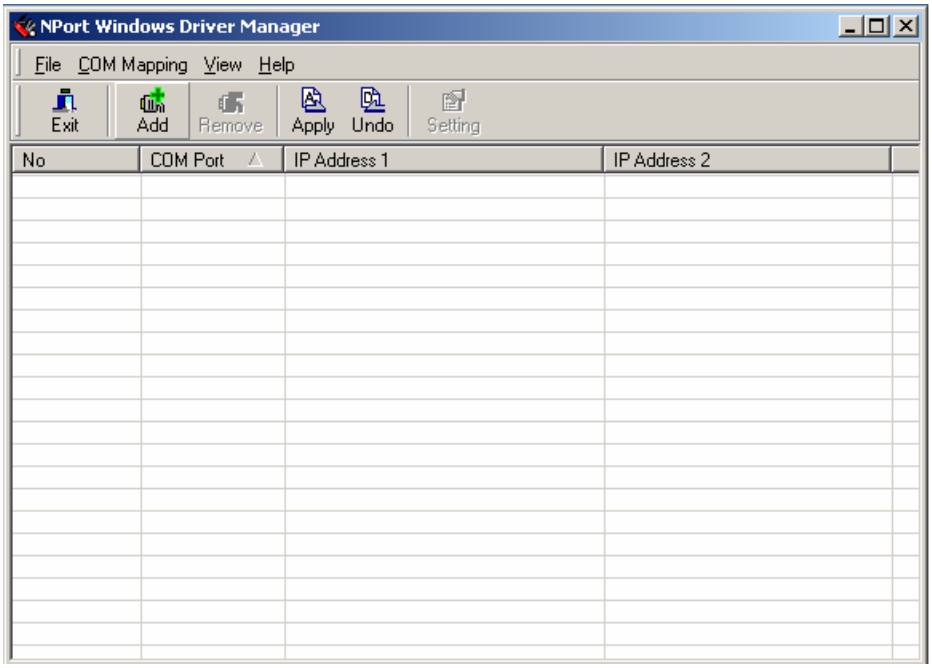
7. Click **Finish** to complete the installation of the CN2600 Windows Driver Manager.


Setup - NPort Windows Driver Manager
Completing the NPort Windows Driver Manager Setup Wizard
Setup has finished installing NPort Windows Driver Manager on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch NPort Windows Driver Manager
Finish

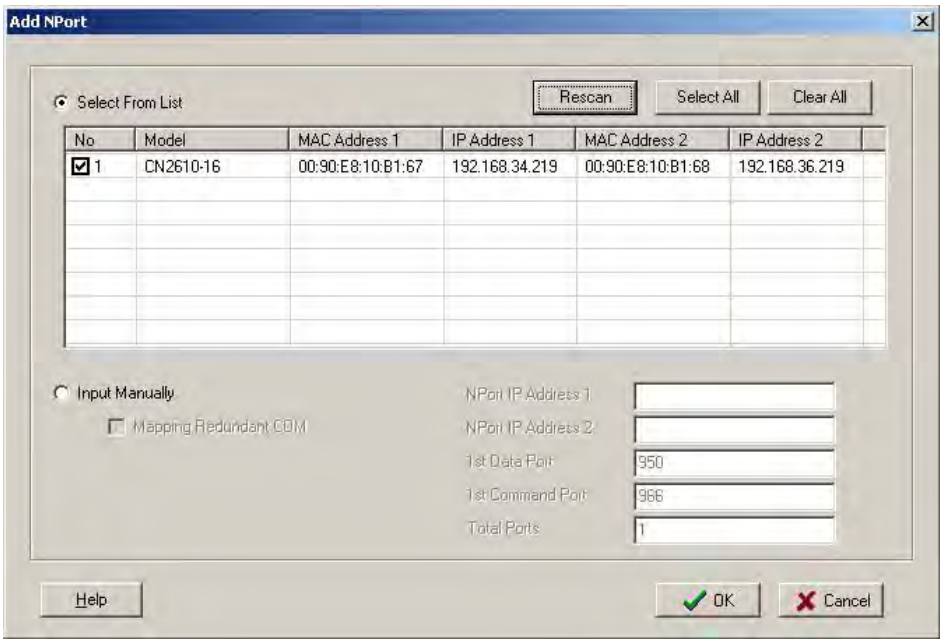
Using NPort Windows Driver Manager

After you install the NPort Windows Driver Manager, you can set up the CN2600's serial ports as remote COM ports for your PC host. Be sure the serial port(s) on your CN2600 are set to **Redundant COM** mode when using NPort Windows Driver Manager to map COM ports.

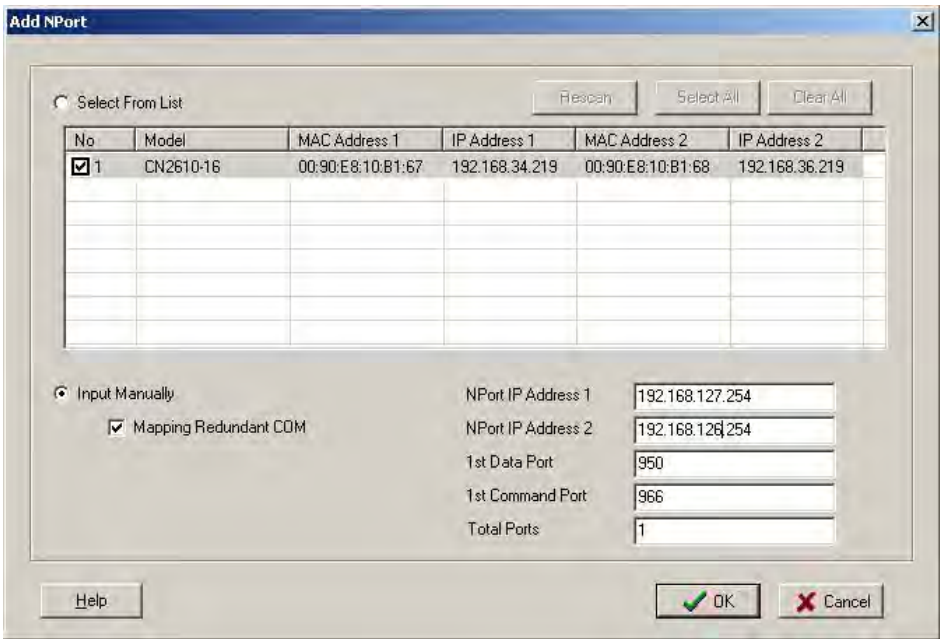
1. Go to **Start → CN2600 series Windows Driver Manager → CN2600 series Windows Driver Manager** to start the COM mapping utility.
2. Click the **Add** icon.



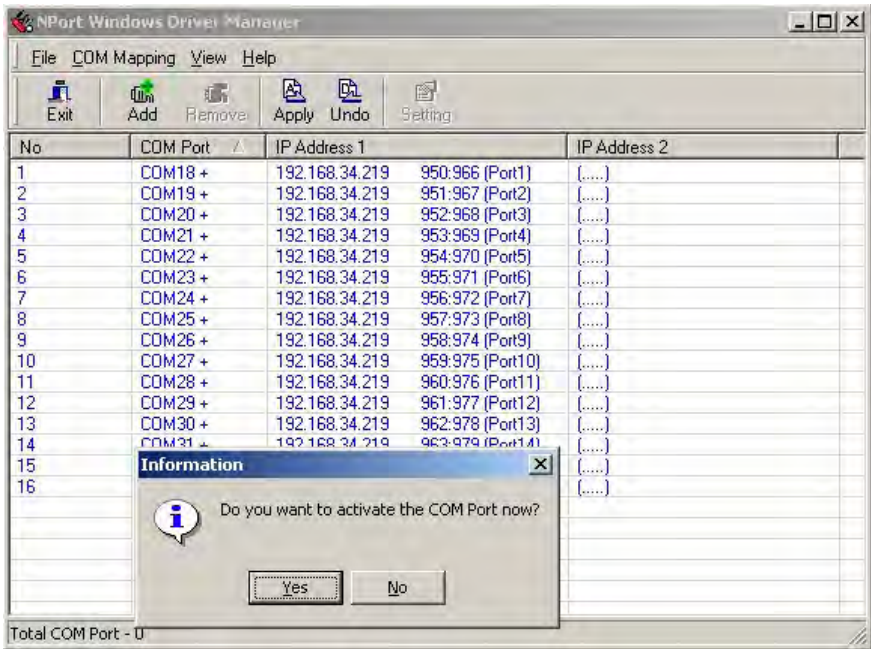
3. Click **Rescan** to search for CN2600 terminal servers. From the list that is generated, select the server that COM ports will be mapped to, and then click **OK**.



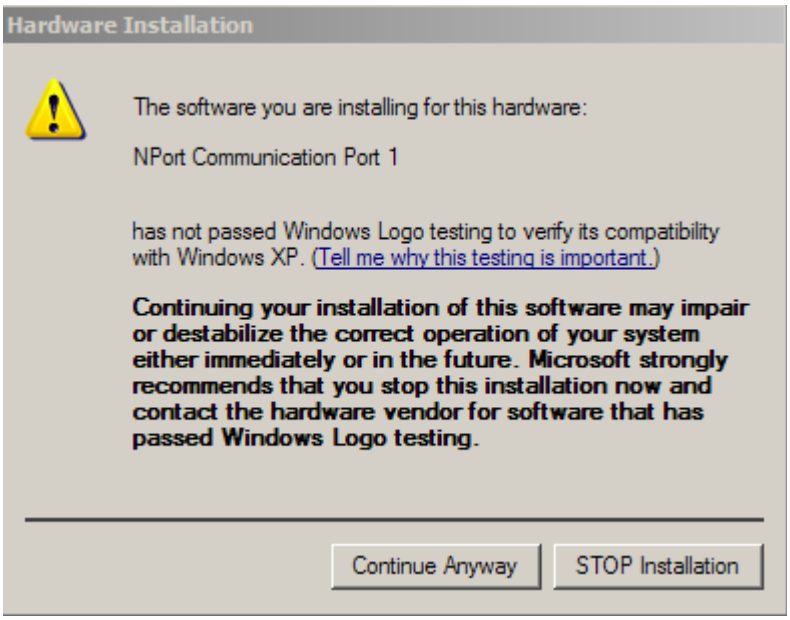
Alternatively, you can select **Input Manually** and then manually enter the CN2600's **IP Address**, **1st Data Port**, **1st Command Port**, and **Total Ports** for the COM ports that will be mapped to. Click **OK** to proceed to the next step. Note that the **Add NPort** page supports FQDN (Fully Qualified Domain Name), in which case the IP address will be filled in automatically.



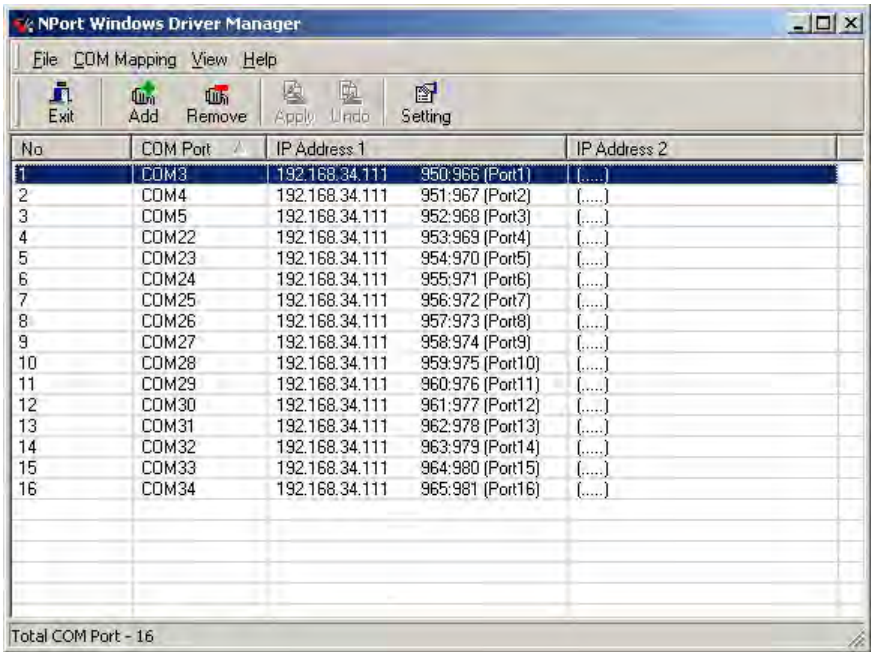
4. COM ports and their mappings will appear in blue until they are activated. Activating the COM ports saves the information in the host system registry and makes the COM port available for use. The host computer will not be able to use the COM ports until the COM ports are activated. Click **Yes** to activate the COM ports at this time, or click **No** to activate the COM ports later.



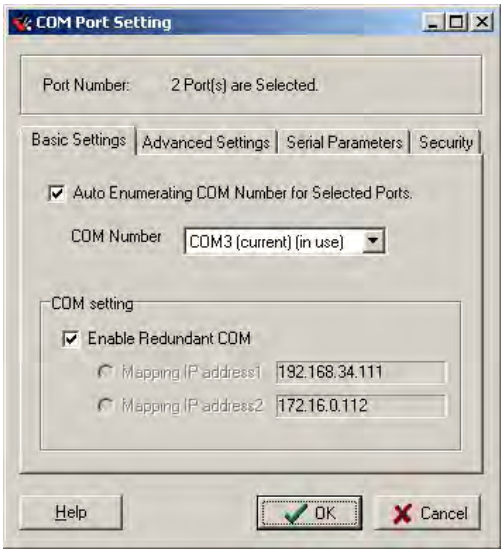
5. In Windows XP, a message is displayed during activation of each port indicating that the software has not passed Windows Logo certification. Click **Continue Anyway** to proceed.


Hardware Installation
The software you are installing for this hardware:
NPort Communication Port 1
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation

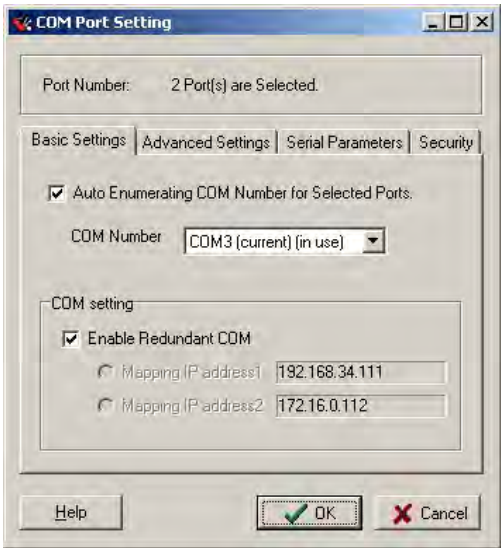
6. Ports that have been activated will appear in black.



To re-configure the settings for a particular serial port on the CN2600, select the row corresponding to the desired port, and then click the **Settings** icon.


COM Port Setting
Port Number: 2 Port(s) are Selected.
Basic Settings Advanced Settings Serial Parameters Security
Auto Enumerating COM Number for Selected Ports.
COM Number COM3 (current) (in use)
COM setting
Enable Redundant COM
Mapping IP address1 192.168.34.111
Mapping IP address2 172.16.0.112
Help OK Cancel

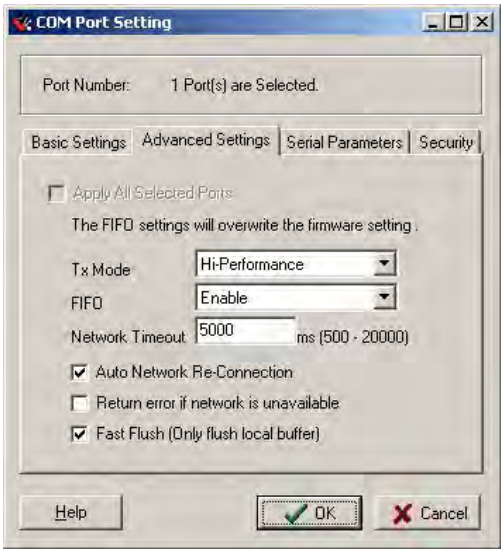
7. On the **Basic Settings** page, use the **COM Number** drop-down list to select a COM number to be assigned to the CN2600 serial port that is being configured. Select the **Auto Enumerating COM Number for Selected Ports** option to assign available COM numbers automatically in sequence to selected serial ports. Note that ports that are "in use" will be labeled accordingly.



8. **Enable Redundant COM**, which enables the 2 LANs automatically, is the default. If **Disable Redundant COM** is selected, Real COM mode will be used, and either LAN can be selected for mapping the IP address.

NOTE Before configuring the driver for "Redundant COM" mode, you must first configure the corresponding port of the CN2600's firmware for "Redundant COM" mode.

9. Click the **Advanced Settings** tab to modify **Tx Mode**, **FIFO**, and **Flash Flush**.



Tx Mode

Hi-Performance is the default for Tx mode. After the driver sends data to the CN2600, the driver immediately issues a "Tx Empty" response to the program. Under **Classical mode**, the driver will not send the "Tx Empty" response until after confirmation is received from the CN2600's serial port. This causes lower throughput. Classical mode is recommended if you want to ensure that all data is sent out before further processing.

FIFO

If **FIFO** is **Disabled**, the CN2600 will transmit one byte each time the Tx FIFO becomes empty, and an Rx interrupt will be generated for each incoming byte. This will result in a faster response and lower throughput.

Network Timeout

You can use this option to prevent blocking if the target CN2600 is unavailable.

Auto Network Re-Connection

With this option enabled, the driver will repeatedly attempt to re-establish the TCP connection if the CN2600 does not respond to background "check alive" packets.

Return error if network is unavailable

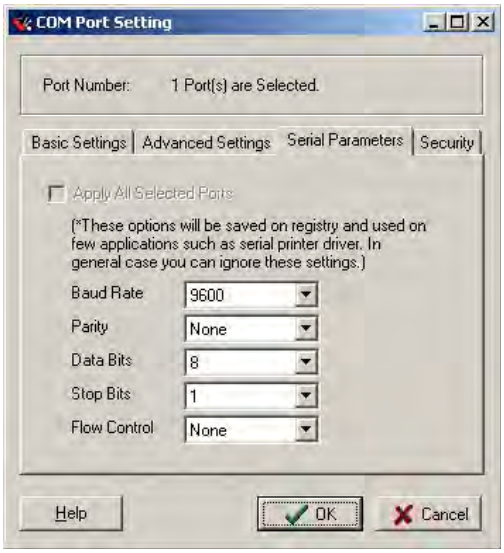
If this option is disabled, the driver will not return any error even when a connection cannot be established to the CN2600. With this option enabled, calling the Win32 Comm function will result in the error return code "STATUS_NETWORK_UNREACHABLE" when a connection cannot be established to the CN2600. This usually means that your host's network connection is down, perhaps due to a cable being disconnected. However, if you can reach other network devices, it may be that the CN2600 is not powered on or is disconnected. Note that **Auto Network Re-Connection** must be enabled in order to use this function.

Fast Flush (only flushes the local buffer)

For some applications, the user's program will use the Win32 "PurgeComm()" function before it reads or writes data. After a program uses this PurgeComm() function, the CN2600 driver will continue to query the CN2600 firmware several times to make sure no data is queued in the CN2600 firmware buffer, rather than just flushing the local buffer. This design is used to satisfy some special considerations. However, it may take more time (on the order of several hundred milliseconds) than a native COM1 due to the additional time spent communicating across the Ethernet. This is why PurgeComm() works significantly faster with native COM ports on the PC than with mapped COM ports on the CN2600. In order to accommodate other applications that require a faster response time, the new CN2600 driver implements a new Fast Flush option. By default, this function is enabled.

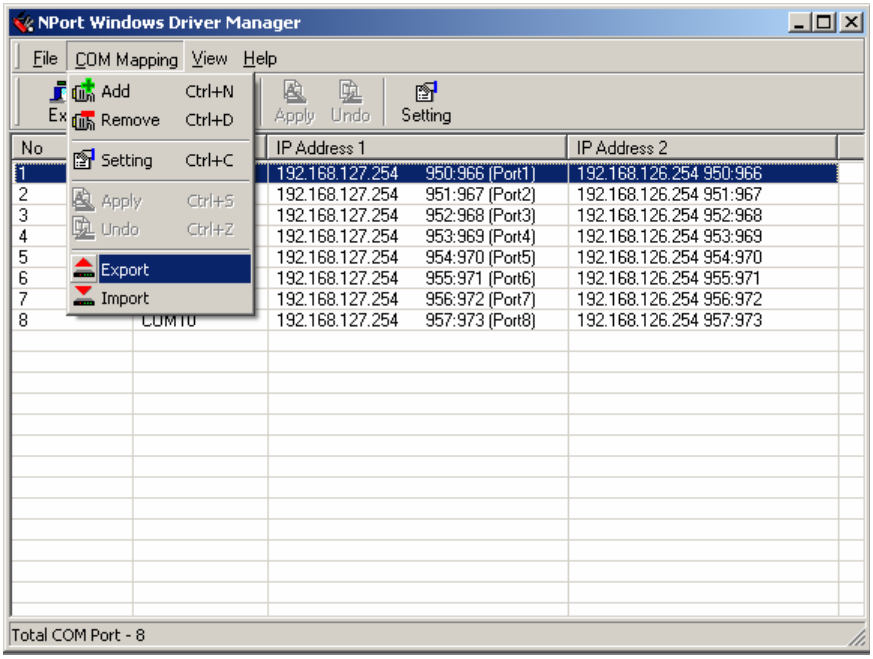
If you have disabled Fast Flush and find that COM ports mapped to the CN2600 perform markedly slower than when using a native COM port, try to verify if "PurgeComm()" functions are used in your application. If so, try enabling the Fast Flush function and see if there is a significant improvement in performance.

10. The **Serial Parameters** page shown in the following figure shows the default settings when the CN2600 is powered on. However, the program can redefine the serial parameters to different values after the program opens the port via Win 32 API.



11. Click the **Security** tab to configure security settings. Select the **Enable Data Encryption** option to enable data to be encrypted when transmitted over the COM ports. After selecting the encryption option, select the **Keep connection** option to start encrypting COM port communications immediately without restarting the COM ports. (If your application will open/close a COM port frequently and the CN2600 is only used for one host, you can enable this option to speed up the opening/closing time. However, this will result in your host tying up the COM port so that other hosts cannot use it.) Select the **Apply All Selected Ports** option to enable the security settings to be applied to all COM ports.

12. To save the configuration to a text file, select Export from the **COM Mapping** menu. You will then be able to import this configuration file to another host and use the same COM Mapping settings in the other host.



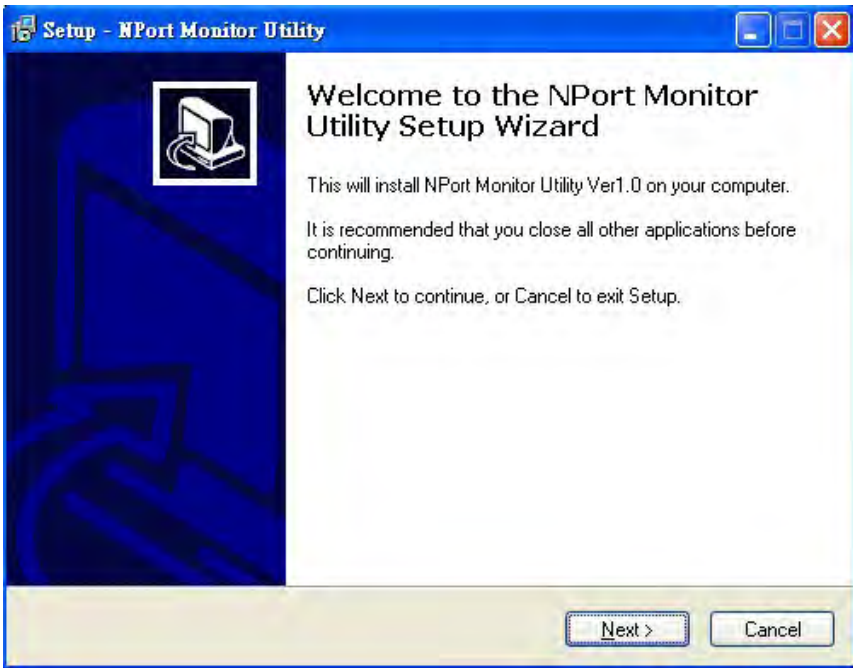
Windows Monitor Utility

Installing the NPort Monitor Utility

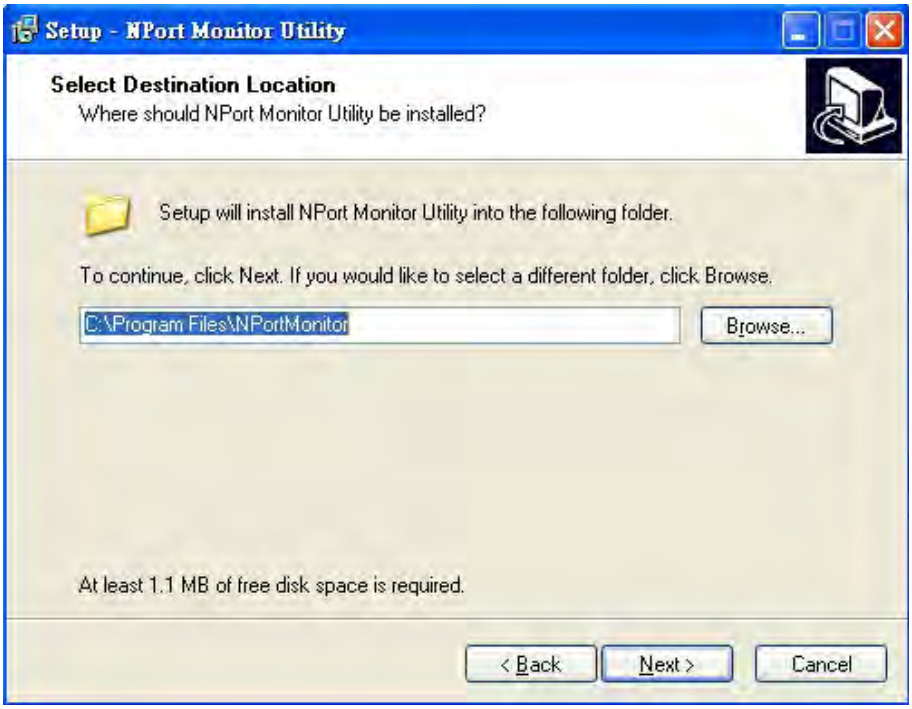
The NPort Monitor Utility is used to monitor the status of redundant COM mode connections. The utility is designed for use with Windows 95/98/ME/NT/2000/XP/2003/Vista.

1. Click the INSTALL Monitor Utility button in the CN2600 Installation CD auto-run window to install the NPort Monitor Utility. Once the installation program starts running, click **Yes** to proceed.

2. Click **Next** when the Welcome screen opens to proceed with the installation.


Setup - NPort Monitor Utility
Welcome to the NPort Monitor Utility Setup Wizard
This will install NPort Monitor Utility Ver1.0 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

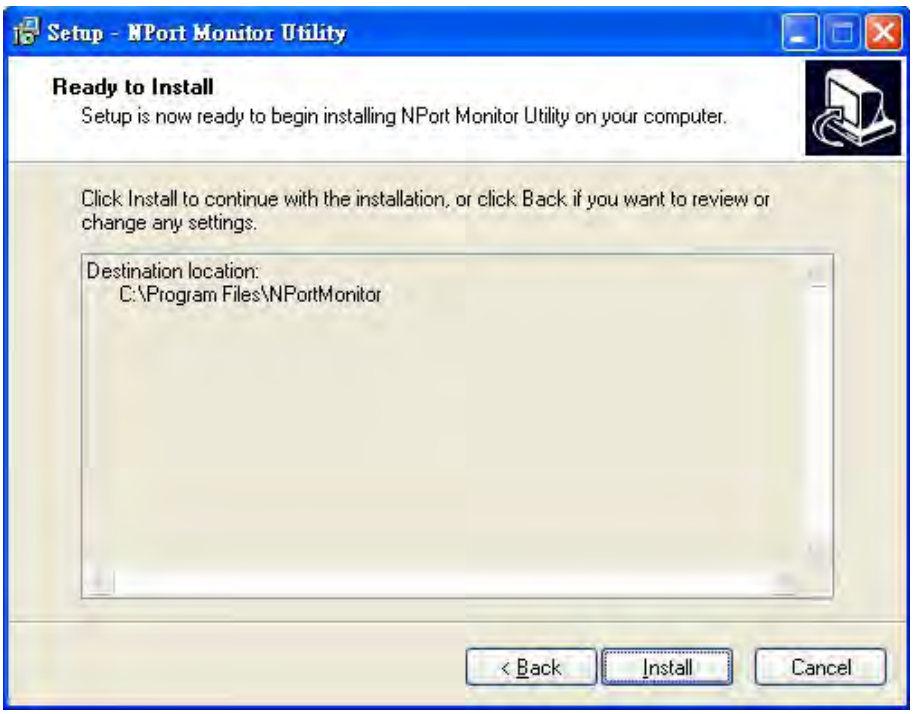
3. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.


Setup - NPort Monitor Utility
Select Destination Location
Where should NPort Monitor Utility be installed?
Setup will install NPort Monitor Utility into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\NPortMonitor
Browse...
At least 1.1 MB of free disk space is required.
< Back
Next >
Cancel

4. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.

Setup - NPort Monitor Utility
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing NPort Monitor Utility, then click Next.
Additional icons:
Create a desktop icon
< Back
Next >
Cancel

5. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.


Setup - NPort Monitor Utility
Ready to Install
Setup is now ready to begin installing NPort Monitor Utility on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\NPortMonitor
< Back
Install
Cancel

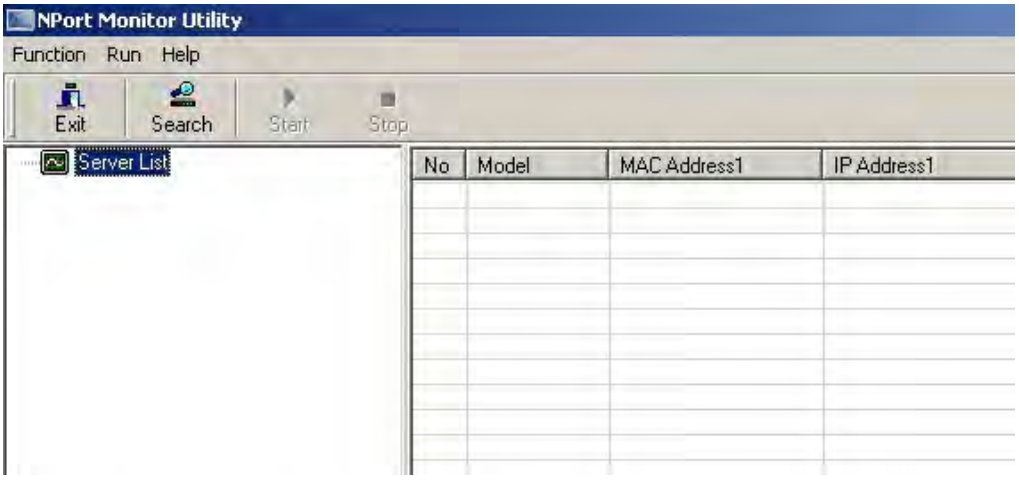
6. Click **Finish** to complete the installation of the NPort Monitor Utility.

Setup - NPort Monitor Utility
Completing the NPort Monitor Utility Setup Wizard
Setup has finished installing NPort Monitor Utility on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch NPort Monitor Utility
Finish

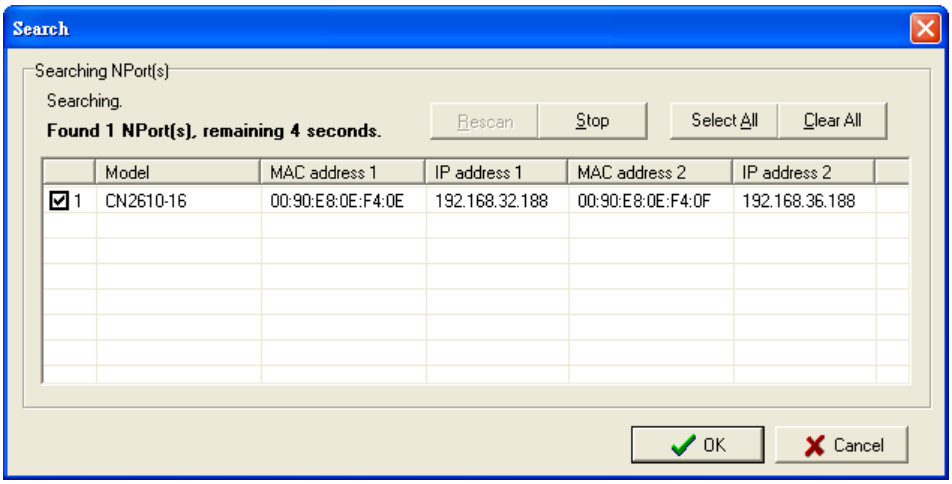
Using the NPort Monitor Utility

After you install the NPort Monitor Utility, you can monitor the status of the IP address and MAC address for redundant LAN 1, and also for redundant LAN 2.

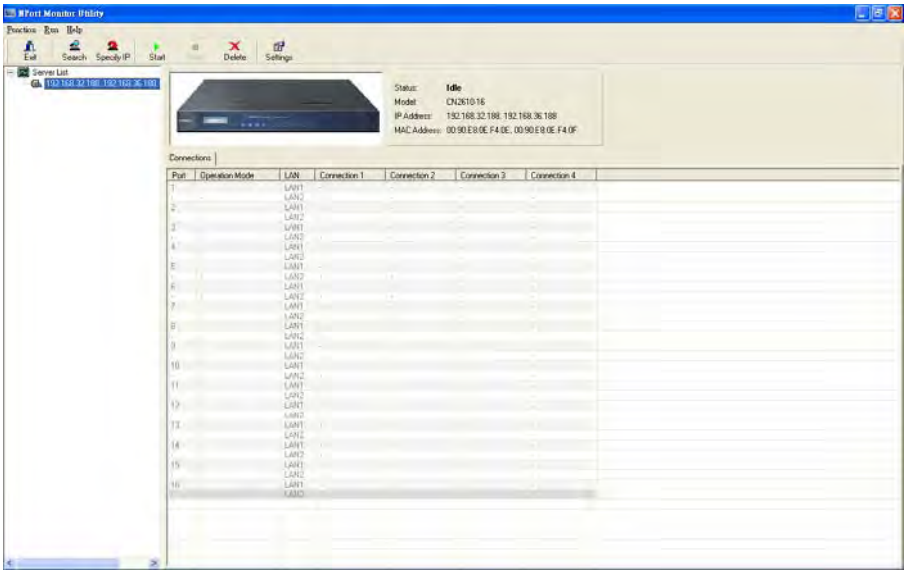
1. Go to **Start → NPort Monitor Utility** to start the monitor utility.
2. Click the **Search** icon.



3. Click **Rescan** to search for CN2600 terminal servers. From the list that is generated, select the server that you will monitor, and then click **OK**.

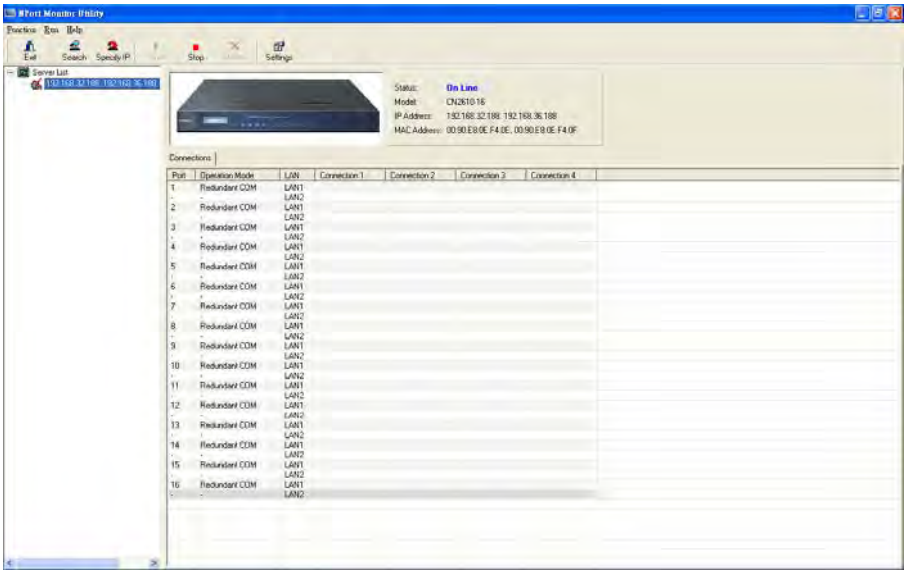


4. The monitoring information will appear on the **Monitoring** page. Select the IP address (from the left hand side) that you would like to monitor, and then click the **Start** icon.



5. The status will be listed as **On Line**, which means that all of the port numbers with LAN 1 and LAN 2 IP addresses will appear on the page.

   If your maximum connections is 2, the monitor's connection 2 will show the LAN IP address.



Linux Real TTY Drivers

Basic Procedures

Follow these instructions to map a CN2600 serial port to a Linux host's tty port:

1. Set up the CN2600. After verifying that the IP configuration works and you can access the CN2600 (by using ping, telnet, etc.), configure the desired serial port on the CN2600 to Real COM mode.
2. Install the Linux Real tty driver files on the host.
3. Map the NPort serial port to the host's tty port.

Hardware Setup

Before proceeding with the software installation, make sure you have completed the hardware installation. Note that the default IP address for the CN2600 is **192.168.127.254**.

NOTE	After installing the hardware, you must configure the operation mode of the serial port on your CN2600 to Real COM mode.

Installing Linux Real TTY Driver Files

1. Obtain the driver file from the included CD-ROM or the MOXA website, at **http://www.moxa.com**.
2. Log in to the console as a super user (root).
3. Execute **cd /** to go to the root directory.
4. Copy the driver file **npreal2xx.tgz** to the **/** directory.
5. Execute **tar xvfz npreal2xx.tgz** to extract all files into the system.
6. Execute **/tmp/moxa/mxinst**.

   For RedHat AS/ES/WS and Fedora Core1, append an extra argument as follows:
   # **/tmp/moxa/mxinst SP1**

The shell script will install the driver files automatically.

7. After installing the driver, you will be able to see several files in the **/usr/lib/npreal2/driver** folder:

> **mxaddsvr** (Add Server, mapping tty port)
> **mxdelsvr** (Delete Server, un-mapping tty port)
> **mxloadsvr** (Reload Server)
> **mxmknod** (Create device node/tty port)
> **mxrmnod** (Remove device node/tty port)
> **mxuninst** (Remove tty port and driver files)

At this point, you will be ready to map the terminal server serial port to the system tty port.

Mapping TTY Ports

Make sure that you set the operation mode of the desired CN2600 serial port to Real COM mode. After logging in as a super user, enter the directory **/usr/lib/npreal2/driver** and then execute **mxaddsvr** to map the serial port on the target terminal server to the host tty ports. The syntax of the **mxaddsvr** command is as follows:

mxaddsvr [*Terminal Server IP Address*] [*Total Ports*] ([*Data port*] [*Cmd port*])

The **mxaddsvr** command performs the following actions:

1. Modifies **npreal2d.cf**.
2. Creates tty ports in directory /dev with major & minor number configured in **npreal2d.cf**.
3. Restarts the driver.

Mapping tty ports automatically

To map tty ports automatically, you may execute **mxaddsvr** with just the IP address and number of ports, as in the following example:

cd /usr/lib/npreal2/driver
./mxaddsvr 192.168.3.4 16

In this example, 16 tty ports will be added, all with IP 192.168.3.4, with data ports from 950 to 965and command ports from 966 to 981.

Mapping tty ports manually

To map tty ports manually, you may execute **mxaddsvr** and manually specify the data and command ports, as in the following example:

cd /usr/lib/npreal2/driver
./mxaddsvr 192.168.3.4 16 4001 966

In this example, 16 tty ports will be added, all with IP 192.168.3.4, with data ports from 4001 to 4016 and command ports from 966 to 981.

Removing Mapped TTY Ports

After logging in as root, enter the directory **/usr/lib/npreal2/driver** and then execute **mxdelsvr** to delete a server. The syntax of mxdelsvr is:

mxdelsvr [*IP Address*]

Example:

cd /usr/lib/npreal2/driver

./mxdelsvr 192.168.3.4

The following actions are performed when executing **mxdelsvr**:

1. Modify npreal2d.cf.
2. Remove the relevant tty ports in directory **/dev**.
3. Restart the driver.

If the IP address is not provided in the command line, the program will list the installed servers and total ports on the screen. You will need to choose a server from the list for deletion.

Removing Linux Driver Files

A utility is included that will remove all driver files, mapped tty ports, and unload the driver. To do this, you only need to enter the directory **/usr/lib/npreal2/driver**, then execute **mxuninst** to uninstall the driver. This program will perform the following actions:

1. Unload the driver.
2. Delete all files and directories in **/usr/lib/npreal2**
3. Delete directory **/usr/lib/npreal2**
4. Modify the system initializing script file.

The UNIX Fixed TTY Driver

Installing the UNIX Driver

1. Log in to UNIX and create a directory for the MOXA TTY. To create a directory named **/usr/etc**, execute the command:

   # **mkdir –p /usr/etc**

2. Copy **moxattyd.tar** to the directory you created. If you created the **/usr/etc** directory above, then execute the following commands:

   # **cp moxattyd.tar /usr/etc**
   # **cd /usr/etc**

3. Extract the source files from the tar file by executing the command:

   # **tar xvf moxattyd.tar**

   The following files will be extracted:

   README.TXT
   moxattyd.c --- source code
   moxattyd.cf --- an empty configuration file
   Makefile --- makefile
   VERSION.TXT --- fixed tty driver version
   FAQ.TXT

4. Compile and Link

   For SCO UNIX:

   # **make sco**

   For UnixWare 7:

   # **make svr5**

   For UnixWare 2.1.x, SVR4.2:

   # **make svr42**

Configuring the UNIX Driver

Modify the configuration:

The configuration used by the **moxattyd program** is defined in the text file **moxattyd.cf**, which is in the same directory that contains the program **moxattyd**. You may use **vi**, or any text editor to modify the file, as follows:

ttyp1 192.168.1.1 950

For more configuration information, view the file **moxattyd.cf,** which contains detailed descriptions of the various configuration parameters.

NOTE The "Device Name" depends on the OS. See the Device Naming Rule section in README.TXT for more information.

To start the moxattyd daemon after system bootup, add an entry into **/etc/inittab**, with the tty name you configured in **moxattyd.cf**, as in the following example:

ts:2:respawn:/usr/etc/moxattyd/moxattyd –t 1

Device naming rule

For UnixWare 7, UnixWare 2.1.x, and SVR4.2, use:

pts/[*n*]

For all other UNIX operating systems, use:

ttyp[*n*]

Starting moxattyd

Execute the command **init q** or reboot your UNIX operating system.

Adding an additional server

1. Modify the text file **moxattyd.cf** to add an additional server. The user can use **vi** or any text editor to modify the file. For more configuration information, look at the file **moxattyd.cf**, which contains detailed descriptions of the various configuration parameters.
2. Find the process ID (PID) of the program **moxattyd**.
   # **ps -ef | grep moxattyd**
3. Update configuration of **moxattyd** program.
   # **kill -USR1** [*PID*]
   (e.g., if moxattyd PID = 404, **kill -USR1 404**)

   This completes the process of adding an additional server.

A

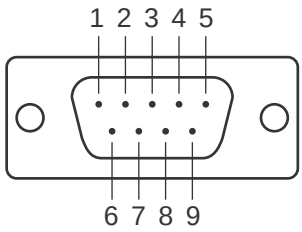
Pinouts and Cable Wiring

This appendix covers the following topics:

- **Port Pinout Diagrams**
  - RS-232/422/485 (Male DB9) Pinouts
  - RS-232 (Male DB9) Pinouts
  - RS-232 (Male RJ45) Pinouts
  - RS-232/422/485 (Male RJ45) Pinouts
- **Cable Wiring Diagrams**
  - Ethernet Cables
  - Serial Cables (RS-232)
  - Serial Cables (RS-422/4-Wire RS-485)
  - Serial Cables (2-Wire RS-485)
  - Pin Assignments for DB9 and DB25 Connectors

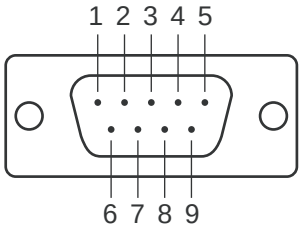
Port Pinout Diagrams

RS-232/422/485 (Male DB9) Pinouts



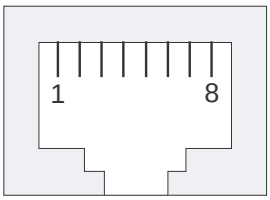
PIN	RS-232	RS-422/ RS-485 (4W)	RS-485 (2W)
1	DCD	TxD-(A)	---
2	RXD	TxD+(B)	---
3	TXD	RxD+(B)	Data+(B)
4	DTR	RxD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	---	---
7	RTS	---	---
8	CTS	---	---
9	---	---	---

RS-232 (Male DB9) Pinouts



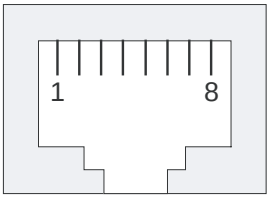
PIN	RS-232
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS

RS-232 (Male RJ45) Pinouts



PIN	RS-232
1	DSR (in)
2	RTS (out)
3	GND
4	TxD (out)
5	RxD (in)
6	DCD (in)
7	CTS (in)
8	DTR (out)

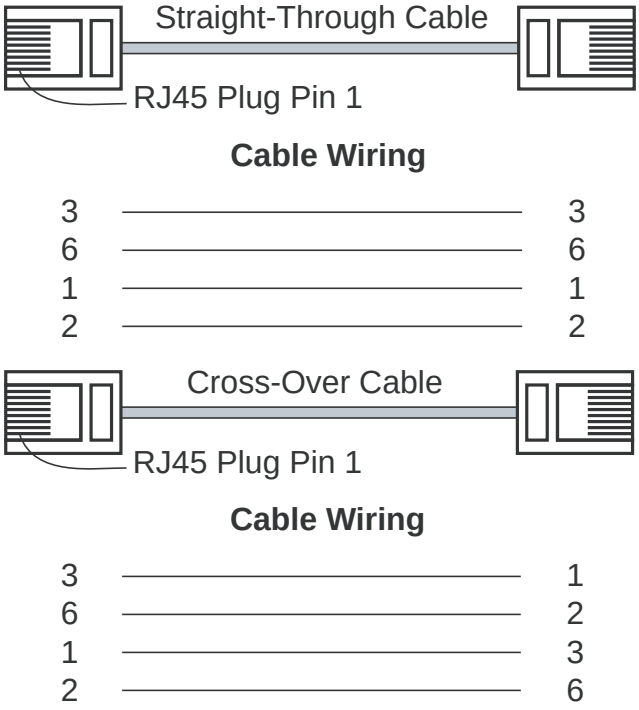
RS-232/422/485 (Male RJ45) Pinouts



PIN	RS-232	RS-422/ RS-485 (4W)	RS-485 (2W)
1	DSR	---	---
2	RTS	TxD+(B)	---
3	GND	GND	GND
4	TXD	TxD-(A)	---
5	RXD	RxD+(B)	Data+(B)
6	DCD	RxD-(A)	Data-(A)
7	CTS	---	---
8	DTR	---	---

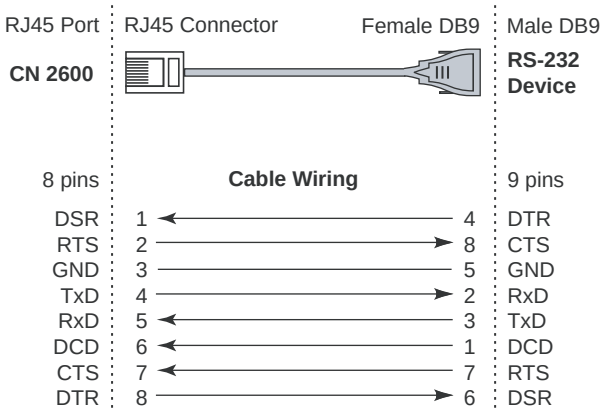
Cable Wiring Diagrams

Ethernet Cables

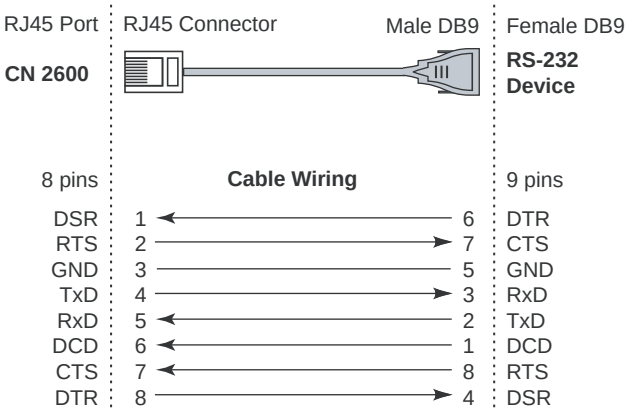


Serial Cables (RS-232)

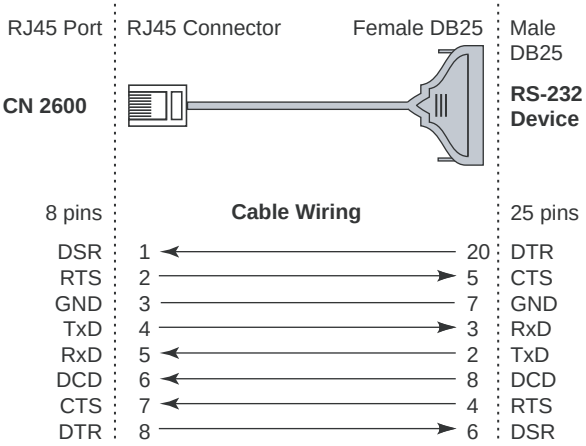
RJ45 (8-pins) to Female DB9



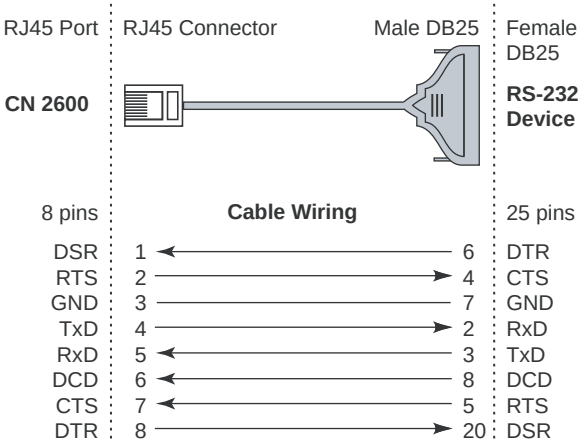
RJ45 (8-pins) to Male DB9



RJ45 (8-pins) to Female DB25

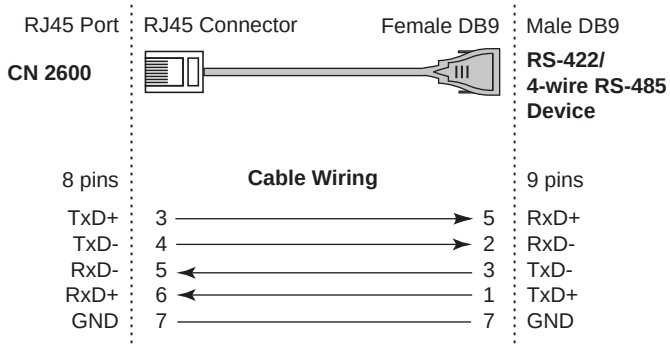


RJ45 (8-pins) to Male DB25

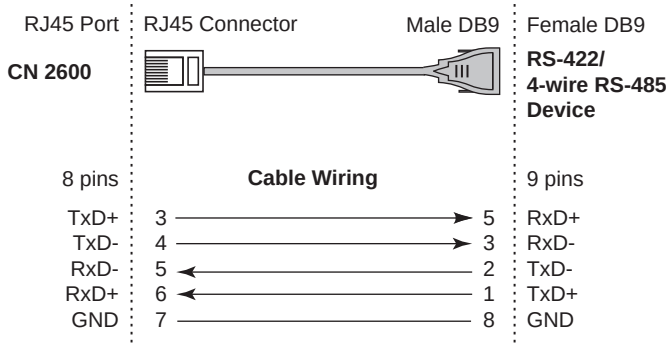


Serial Cables (RS-422/4-Wire RS-485)

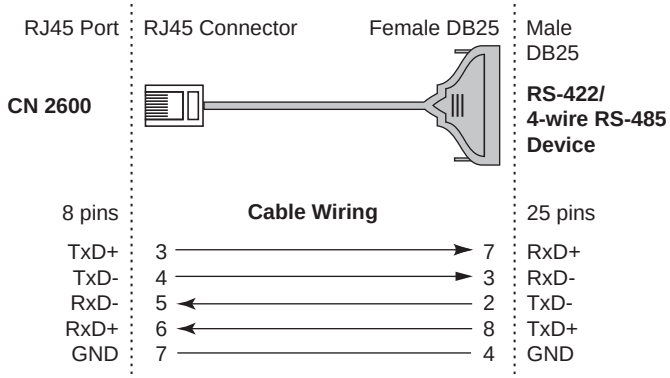
RJ45 (8-pins) to Female DB9



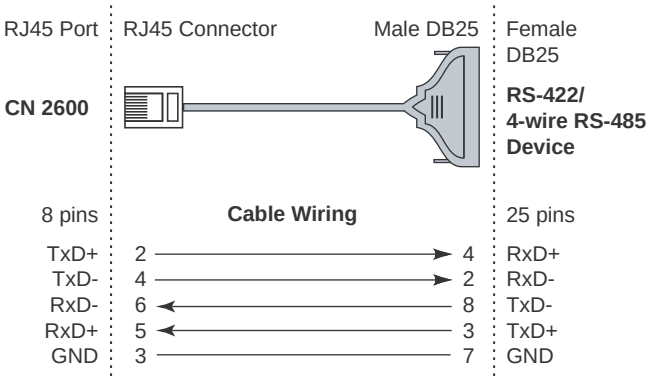
RJ45 (8-pins) to Male DB9



RJ45 (8-pins) to Female DB25

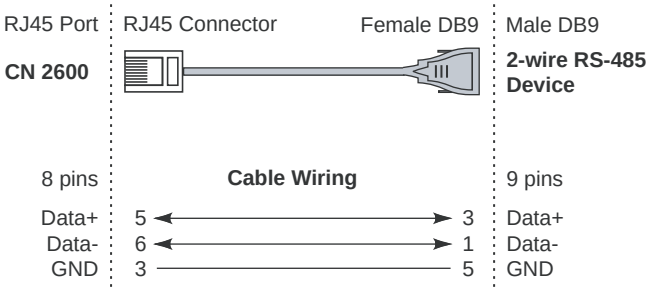


RJ45 (8-pins) to Male DB25

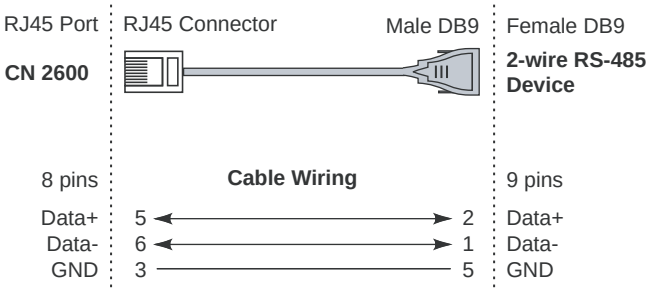


Serial Cables (2-Wire RS-485)

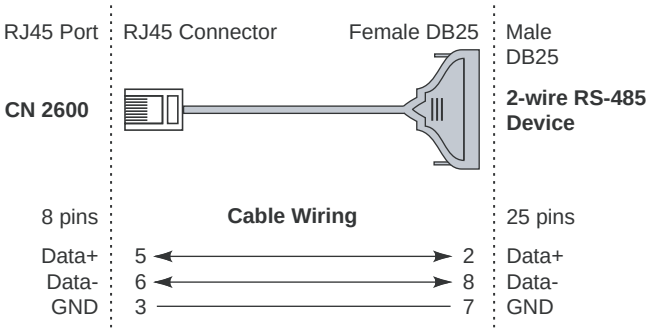
RJ45 (8-pins) to Female DB9



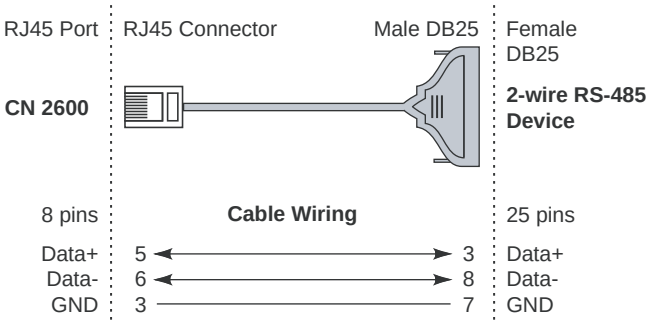
RJ45 (8-pins) to Male DB9



RJ45 (8-pins) to Female DB25



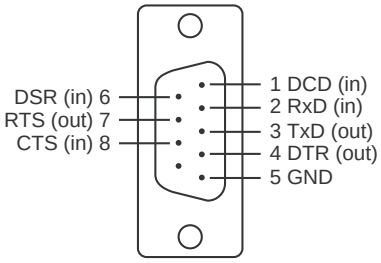
RJ45 (8-pins) to Male DB25



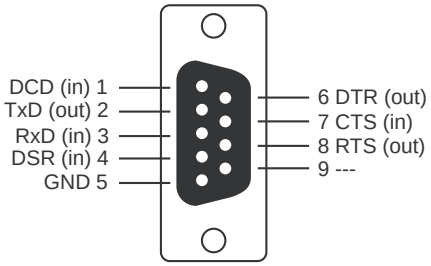
Pin Assignments for DB9 and DB25 Connectors

Pin Assignments for DB9 Male and Female Connectors

DB9 Male Connector

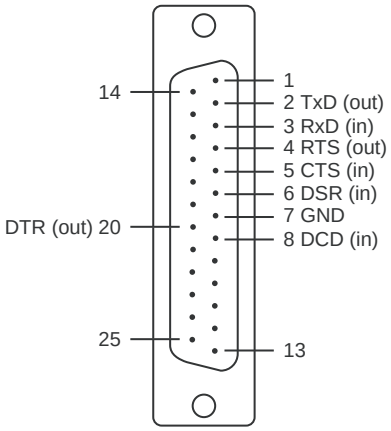


DB9 Female Connector

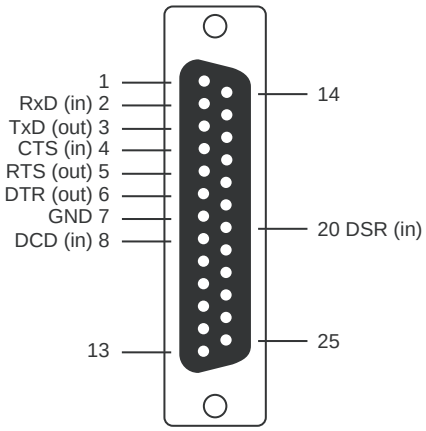


Pin Assignments for DB25 Male and Female Connectors

DB25 Male Connector



DB25 Female Connector



B

SNMP Agent with MIB II

Simple Network Management Protocol agent software is built into the CN2600. The software supports cold/warm start trap, line up/down trap, and RFC 1213 MIB-II. The following table lists the standard MIB-II groups, as well as the variable implementations for the CN2600.

Supported SNMP variables

System MIB	Interfaces MIB	IP MIB	ICMP MIB
SysDescr	itNumber	ipForwarding	IcmpInMsgs
SysObjectID	ifIndex	ipDefaultTTL	IcmpInErrors
SysUpTime	ifDescr	ipInreceives	IcmpInDestUnreachs
SysContact	ifType	ipInHdrErrors	IcmpInTimeExcds
SysName	ifMtu	ipInAddrErrors	IcmpInParmProbs
SysLocation	ifSpeed	ipForwDatagrams	IcmpInSrcQuenchs
SysServices	ifPhysAddress	ipInUnknownProtos	IcmpInRedirects
	ifAdminStatus	ipInDiscards	IcmpInEchos
	ifOperStatus	ipInDelivers	IcmpInEchoReps
	ifLastChange	ipOutRequests	IcmpInTimestamps
	ifInOctets	ipOutDiscards	IcmpTimestampReps
	ifInUcastPkts	ipOutNoRoutes	IcmpInAddrMasks
	ifInNUcastPkts	ipReasmTimeout	IcmpOutMsgs
	ifInDiscards	ipReasmReqds	IcmpOutErrors
	ifInErrors	ipReasmOKs	IcmpOutDestUnreachs
	ifInUnknownProtos	ipReasmFails	IcmpOutTimeExcds
	ifOutOctets	ipFragOKs	IcmpOutParmProbs
	ifOutUcastPkts	ipFragFails	IcmpOutSrcQuenchs
	ifOutNUcastPkts	ipFragCreates	IcmpOutRedirects
	ifOutDiscards	ipAdEntAddr	IcmpOutEchos
	ifOutErrors	ipAdEntIfIndex	IcmpOutEchoReps
	ifOutQLen	ipAdEntNetMask	IcmpOutTimestamps
	ifSpecific	ipAdEntBcastAddr	IcmpOutTimestampReps
		ipAdEntReasmMaxSize	IcmpOutAddrMasks
		IpNetToMediaIfIndex	IcmpOutAddrMaskReps
		IpNetToMediaPhysAddress	
		IpNetToMediaNetAddress	
		IpNetToMediaType	
		IpRoutingDiscards	

UDP MIB	TCP MIB	SNMP MIB
UdpInDatagrams	tcpRtoAlgorithm	snmpInPkts
UdpNoPorts	tcpRtoMin	snmpOutPkts
UdpInErrors	tcpRtoMax	snmpInBadVersions
UdpOutDatagrams	tcpMaxConn	snmpInBadCommunityNames
UdpLocalAddress	tcpActiveOpens	snmpInASNParseErrs
UdpLocalPort	tcpPassiveOpens	snmpInTooBigs
	tcpAttempFails	snmpInNoSuchNames
Address Translation MIB	tcpEstabResets	snmpInBadValues
AtIfIndex	tcpCurrEstab	snmpInReadOnlys
AtPhysAddress	tcpInSegs	snmpInGenErrs
AtNetAddress	tcpOutSegs	snmpInTotalReqVars
	tcpRetransSegs	snmpInTotalSetVars
	tcpConnState	snmpInGetRequests
	tcpConnLocalAddress	snmpInGetNexts
	tcpConnLocalPort	snmpInSetRequests
	tcpConnRemAddress	snmpInGetResponses
	tcpConnRemPort	snmpInTraps
	tcpInErrs	snmpOutTooBigs
	tcpOutRsts	snmpOutNoSuchNames
		snmpOutBadValues
		snmpOutGenErrs
		snmpOutGetRequests
		snmpOutGetNexts
		snmpOutSetRequests
		snmpOutGetResponses
		snmpOutTraps
		snmpEnableAuthenTraps

C

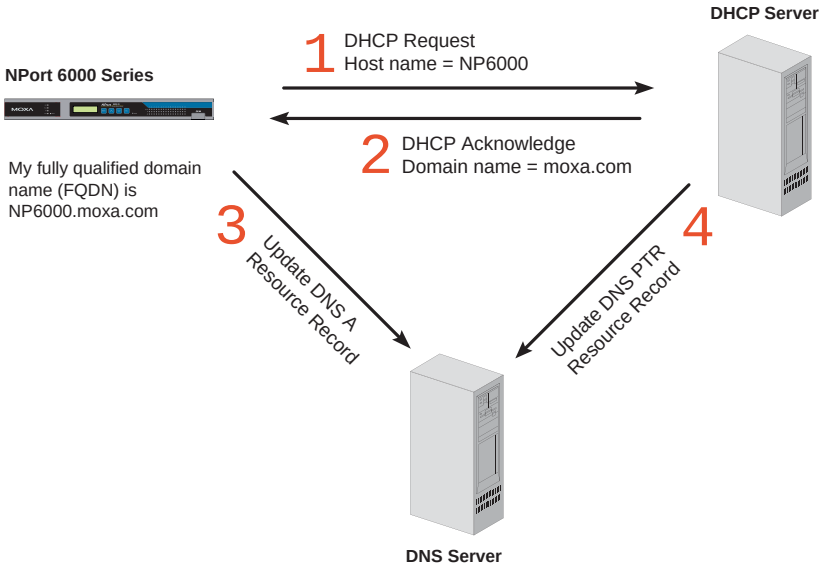
Dynamic Domain Name Server

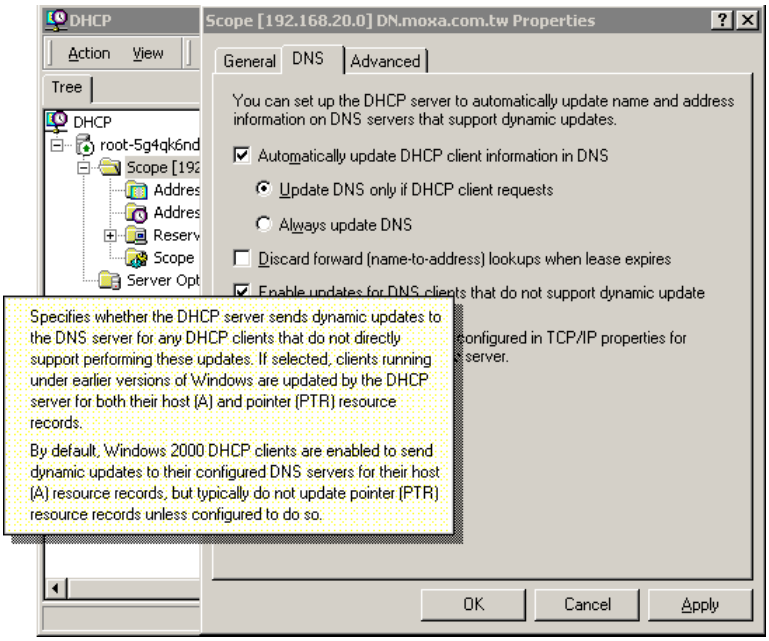
This appendix explains how to use the CN2600 with DDNS. When the CN2600 receive its IP address from a DHCP (Dynamic Host Configuration Protocol) server, remote servers will be unable to access it using a fixed IP address. With DDNS (Dynamic Domain Name Server), a remote server can access the CN2600 using its domain name instead of its IP address.

Overview

The following is a summary of the process:

1. The CN2600 sends a request for an IP address to the DHCP server. At the same time, it notifies the DHCP server of its desired server name (CN2600 in the illustration) according to the option 12 standard.
2. The DHCP server replies with the IP address that is assigned to the CN2600, along with the domain name (“moxa.com” in the illustration) and the IP addresses for the DNS server and gateway.
3. If the CN2600 has authorization to update the DNS server, it will register its FQDN (Fully Qualified Domain Name) with the DNS server. The CN2600’s FQDN will be in the format *server name*.*domain name* (CN2600.moxa.com” in the illustration).
4. If the CN2600 is not authorized to update the DNS server, the DHCP server can be used to update the DNS server. The DHCP server will register the DNS server with the PTR RR (the record of request for a domain name with IP address).

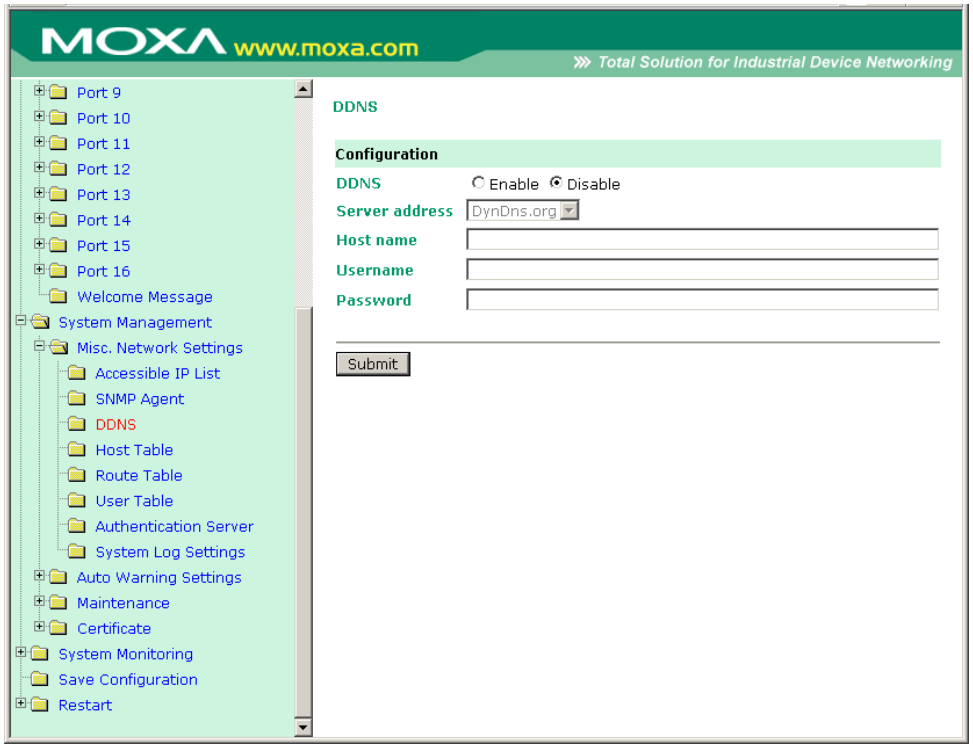



DHCP
Action View
Tree
DHCP
root-5g4qk6nd
Scope [192
Addres
Addres
Reserv
Scope
Server Opt
Scope [192.168.20.0] DN.moxa.com.tw Properties
General DNS Advanced
You can set up the DHCP server to automatically update name and address information on DNS servers that support dynamic updates.
Automatically update DHCP client information in DNS
Update DNS only if DHCP client requests
Always update DNS
Discard forward (name-to-address) lookups when lease expires
Enable updates for DNS clients that do not support dynamic update
Specifies whether the DHCP server sends dynamic updates to the DNS server for any DHCP clients that do not directly support performing these updates. If selected, clients running under earlier versions of Windows are updated by the DHCP server for both their host (A) and pointer (PTR) resource records.
By default, Windows 2000 DHCP clients are enabled to send dynamic updates to their configured DNS servers for their host (A) resource records, but typically do not update pointer (PTR) resource records unless configured to do so.
configured in TCP/IP properties for
server.
OK
Cancel
Apply

The above screenshot shows how DHCP can be set up to update the DNS.

Currently, the CN2600 supports DNS service as provided by DynDNS. For detailed information on this option, please visit https://www.dyndns.com.

Configuration



DDNS (default=Disable):Use this field to enable or disable DDNS.

Server address (default=DynDns.org): Currently, DynDns.org is the only option available for Server address.

Host name: In this field, use the name that you created on www.dyndns.com. The CN2600 will update the DynDNS server with this host name.

Username: This is the user name used for update authentication.

Password: This is the password used for update authentication.

D

Well Known Port Numbers

In this appendix, we provide a list of well known port numbers that may cause network problems if you set the CN2600 to one of these ports. Refer to RFC 1700 for well known port numbers or to the following introduction from the IANA:

The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.

The Well Known Ports range from 0 through 1023.

The Registered Ports range from 1024 through 49151.

The Dynamic and/or Private Ports range from 49152 through 65535.

The Well Known Ports are assigned by the IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. The following table shows famous port numbers among the listed well-known port numbers. For more details, please visit the IANA website at http://www.iana.org/assignments/port-numbers.

TCP Socket	Application Service
0	Reserved
1	TCP Port Service Multiplexer
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
13	Daytime
15	Netstat
20	FTP data port
21	FTP control port
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
37	Time (Time Server)
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (login)

TCP Socket	Application Service
53	Domain Name Server (domain)
79	Finger protocol (finger)
80	World Wide Web (HTTP)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol
213	IPX
160 to 223	Reserved for future use

UDP Socket	Application Service
0	Reserved
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
13	Daytime
35	Any private printer server
39	Resource Location Protocol
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (login)
53	Domain Name Server (domain)
69	Trivial Transfer Protocol (TETP)
70	Gopher Protocol
79	Finger Protocol
80	World Wide Web (HTTP)
107	Remote Telnet Service
111	Sun Remote Procedure Call (Sunrpc)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
161	SNMP (Simple Network Mail Protocol)
162	SNMP Traps
213	IPX (used for IP Tunneling)

E

RADIUS Server

Managing diverse serial lines and modem pools for large numbers of users creates the need for significant administrative support. Since modem pools are links to the outside world, careful attention must be paid to security, authorization, and accounting. This can best be achieved by managing a single database of users allowing authentication (verifying user names and passwords) as well as configuration of information that details the type of service to deliver to the user (e.g. SLIP, PPP, Telnet, and rlogin). The CN2600 supports the RADIUS protocol, which requires only one database for remote user management.

This appendix covers the following topics:

- **What is RADIUS?**
  - Definition
  - Client/Server Architecture
- **Setting up the CN2600**
  - Setting up the RADIUS Server IP Address
  - Serial Port Configuration
- **Setting up UNIX Hosts**
- **Setting up Windows NT Hosts**
- **Setting up Windows 2000 Hosts**
- **Setting up Windows 2003 Hosts**

What is RADIUS?

Definition

Remote Authentication Dial-up User Service, or RADIUS, is the standard for centralizing the authentication, authorization, and accounting of remote access users.

Here is a brief description of how RADIUS works: When a user dials in to a remote access device, that device communicates with the central RADIUS server to determine if the user is authorized to connect to the LAN. The RADIUS server performs the authentication and responds with the result—either accept or reject. If the user is accepted, the remote access server routes the user onto the network; if not, the server will terminate the user's connection. The RADIUS server also provides accounting services if supported by the remote access server.

With RADIUS, a network manager or ISP only needs to maintain a single, central database against which all remote user authentications take place. This greatly eases the management burden associated with administering a large number of dial-in users.

Client/Server Architecture

RADIUS is a type of client-server software. Communication servers such as the CN2600 play an active role, whereas RADIUS servers are passive.

When a remote host is connected to the CN2600, the host is prompted to enter a user ID and password.

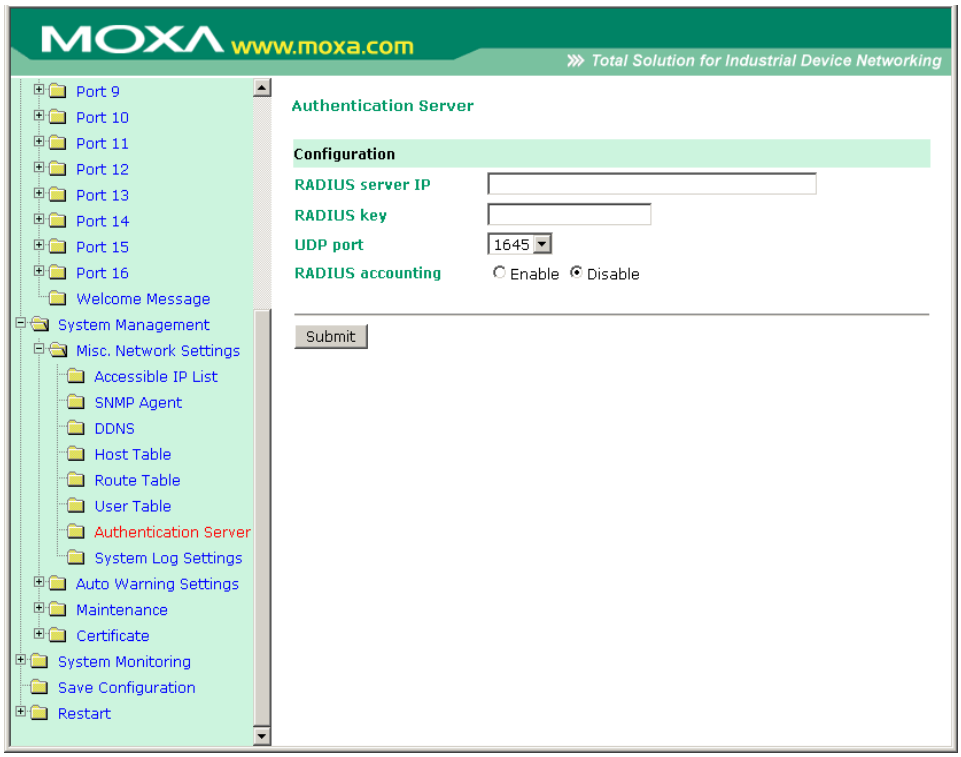
After receiving the user ID and password, the CN2600 sends the information to a defined RADIUS server. Up to this point, the remote user is still unable to access the network.

The RADIUS server compares the user ID and password with its internal database and responds through the network, either accepting or rejecting the connection attempt.

If the CN2600 receives the "accept" message from the RADIUS server, the remote user is allowed to access the network. Otherwise, the CN2600 will either terminate the connection or attempt to connect again after a specified duration of time.

Setting up the CN2600

Setting up the RADIUS Server IP Address



RADIUS server IP: This is the IP address of the RADIUS server.

RADIUS key: This is the password that is used to access the RADIUS server IUS server

UDP port: This is the RADIUS server's assigned UDP port.

RADIUS accounting: This field enables or disables RADIUS accounting.

Serial Port Configuration

RADIUS is an effective authentication method for dial-up services. In addition to dial-up services (PPP, SLIP, and Dynamic), the CN2600 supports RADIUS settings for terminal applications and console management application. You will see it as an option for **Authentication type** when configuring the port's operation mode. Please refer to Chapter 7, Configuring Serial Port Operation Mode, for detailed information and configuration instructions

Setting up UNIX Hosts

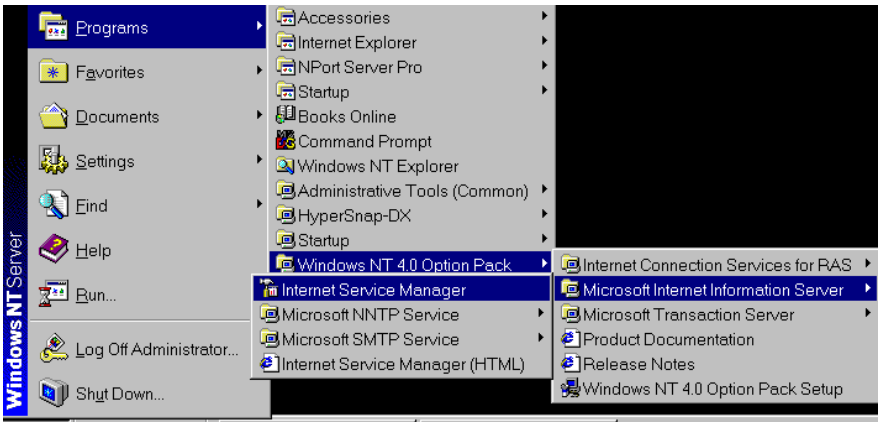
MOXA recommends the FreeRADIUS server for UNIX users. FreeRADIUS is the premiere open-source RADIUS server and is one of the top five RADIUS servers in use world-wide. It is effective for both embedded systems with small amounts of memory and for systems with millions of users. It is fast, flexible, and configurable, and it supports more authentication protocols than many commercial servers.

The server is released under the GNU General Public License (GPL), which means that it is free to download and install. FreeRADIUS can be downloaded from the following website:

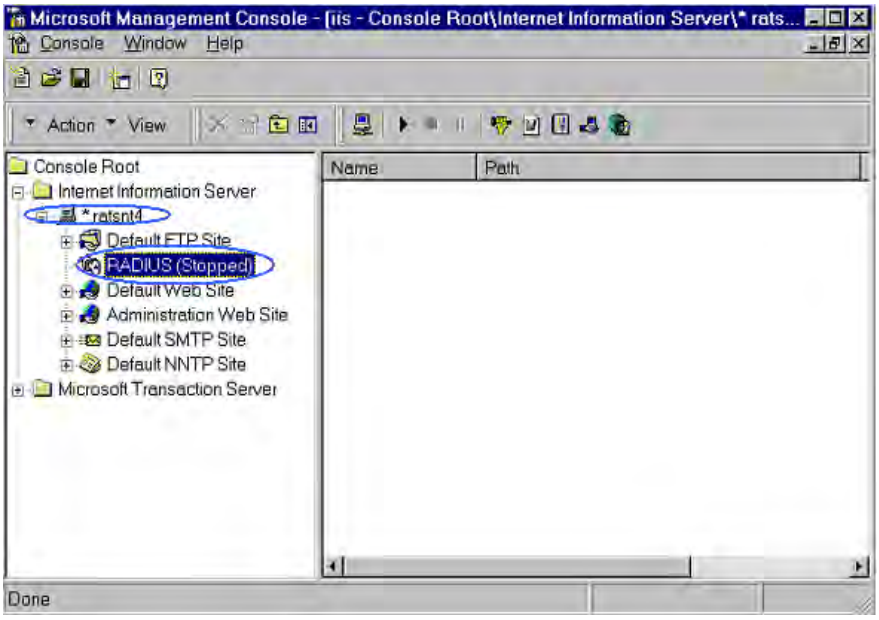
http://www.freeradius.com/

Setting up Windows NT Hosts

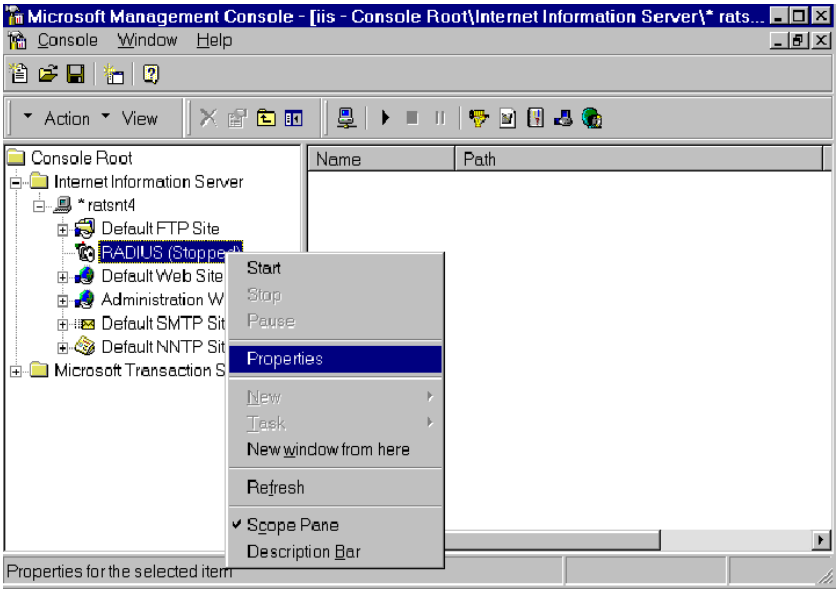
1. Install Windows NT OPTION PACK 4.0 on the Windows NT server.
2. Open **Start → Programs → Windows NT 4.0 Option Pack → Microsoft Internet Information Server → Management Console Manger**.



3. Go to **Console Root → Internet Information Server** (in the left pane). Your computer's name should be visible.
4. Find your computer's name in the left panel and click on it, after which you will see RADIUS in the right information window.

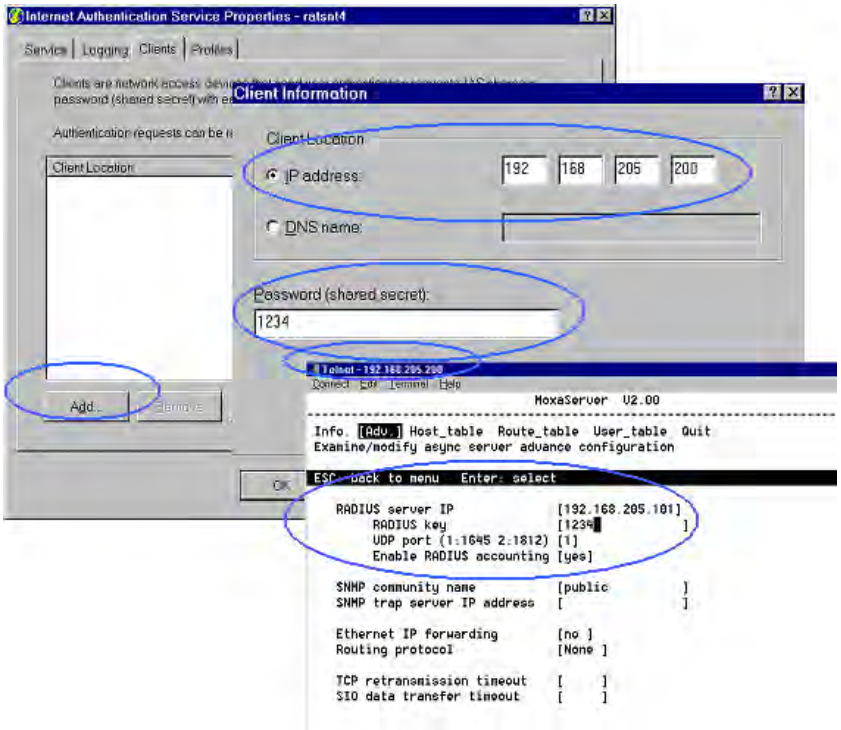


5. Right click **RADIUS** in the left information window, and then select **Properties**.



6. Select **Service**. Verify that the RADIUS ports assignments match your configuration.
   [Authentication] 1645 or 1812
   [Accounting] 1646 or 1813

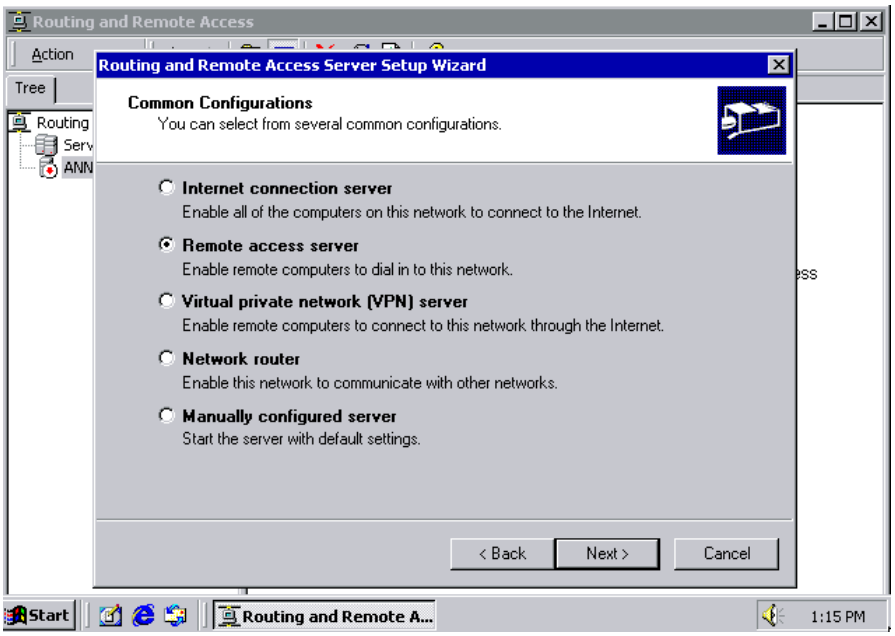
7. Select **Client**, and then click **Add**. Enter the CN2600's IP address in the IP address field. Enter the CN2600's RADIUS key in the password field. This must match the RADIUS key that you set in the CN2600 console.


Internet Authentication Service Properties - ratsnt4
Service Logging Clients Profiles
Client Information
Client Location
IP address:
192 168 205 200
DNS name:
Password (shared secret):
1234
Add...
MoxaServer V2.00
Info. [Adv.] Host_table Route_table User_table Quit
Examine/modify async server advance configuration
ESC: back to menu Enter: select
RADIUS server IP [192.168.205.101]
RADIUS key [1234]
UDP port (1:1645 2:1812) [1]
Enable RADIUS accounting [yes]
SNMP community name [public]
SNMP trap server IP address [ ]
Ethernet IP forwarding [no]
Routing protocol [None]
TCP retransmission timeout [ ]
SIO data transfer timeout [ ]

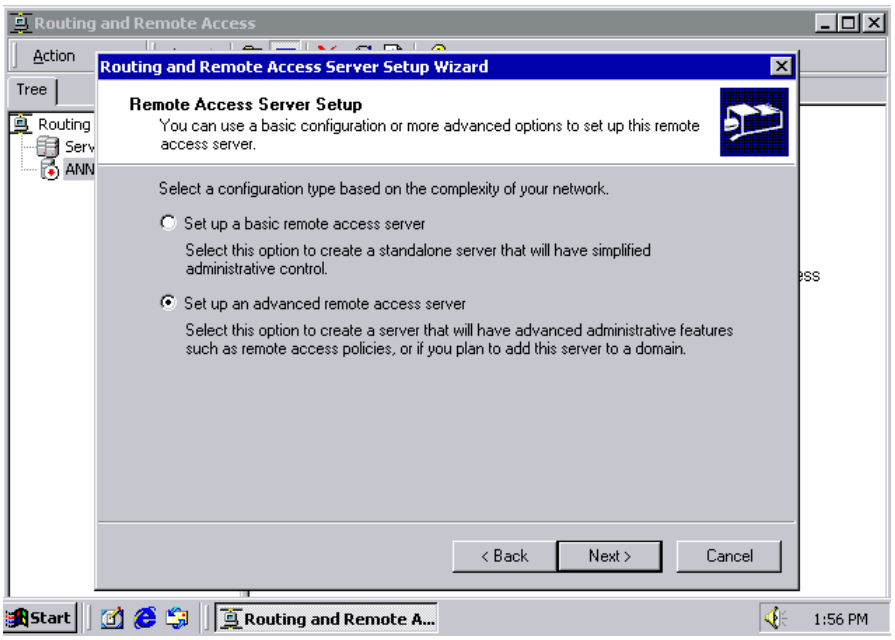
8. Click **Apply**.
9. Right click **RADIUS** in the left information window, and select **Start**. You will now see that RADIUS is running.

Setting up Windows 2000 Hosts

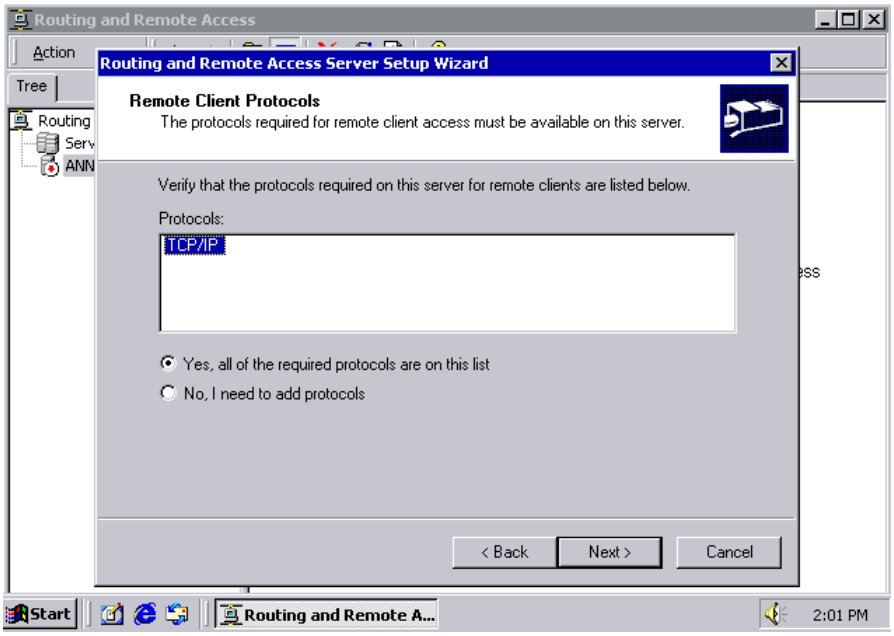
1. Open **Start → Programs → Administrative Tools → Routing and Remote Access**.
2. Right click **Server (Local)** and select **Configure** and **Enable Routing and Remote Access**. Click **Next** to continue.
3. Select **Remote access server** and click **Next** to continue.


Routing and Remote Access
Action
Tree
Routing and Remote Access Server Setup Wizard
Common Configurations
You can select from several common configurations.
Internet connection server
Enable all of the computers on this network to connect to the Internet.
Remote access server
Enable remote computers to dial in to this network.
Virtual private network (VPN) server
Enable remote computers to connect to this network through the Internet.
Network router
Enable this network to communicate with other networks.
Manually configured server
Start the server with default settings.
< Back
Next >
Cancel
Start
Routing and Remote A...
1:15 PM

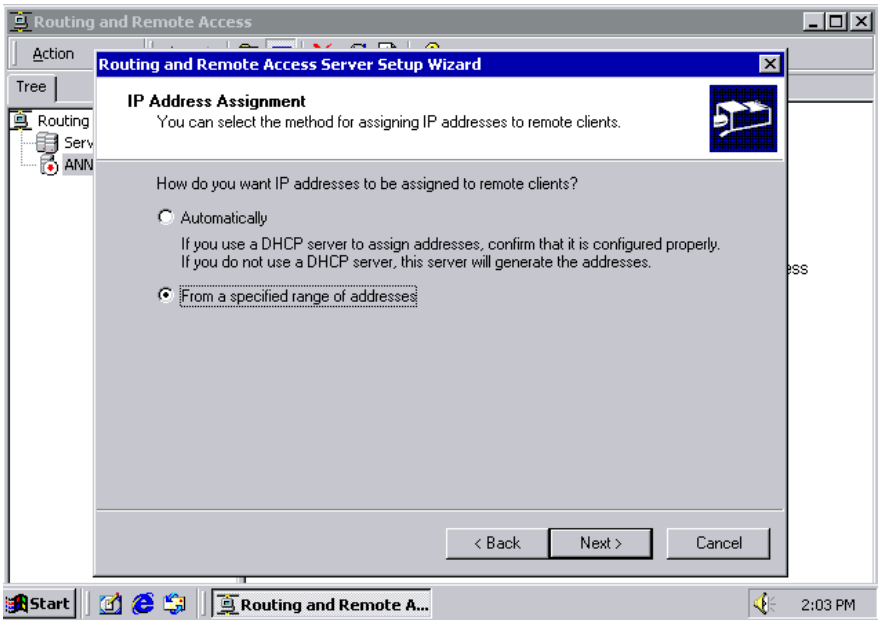
4. Select **Set up an advanced remote access server** and click **Next** to continue.

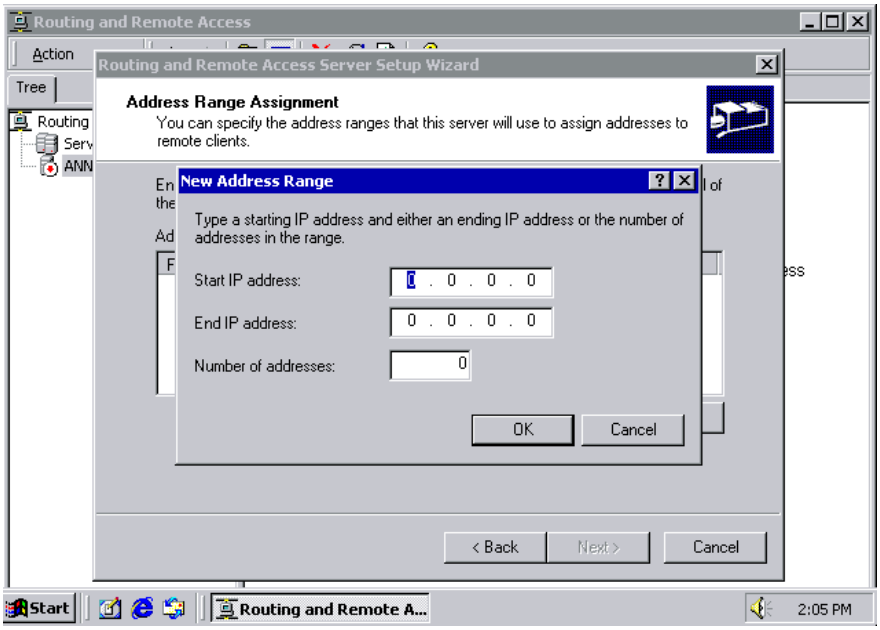

Routing and Remote Access
Action
Tree
Routing and Remote Access Server Setup Wizard
Remote Access Server Setup
You can use a basic configuration or more advanced options to set up this remote access server.
Select a configuration type based on the complexity of your network.
Set up a basic remote access server
Select this option to create a standalone server that will have simplified administrative control.
Set up an advanced remote access server
Select this option to create a server that will have advanced administrative features such as remote access policies, or if you plan to add this server to a domain.
< Back
Next >
Cancel
Start
Routing and Remote A...
1:56 PM

5. Select **TCP/IP protocol**, then click **Next** to continue.

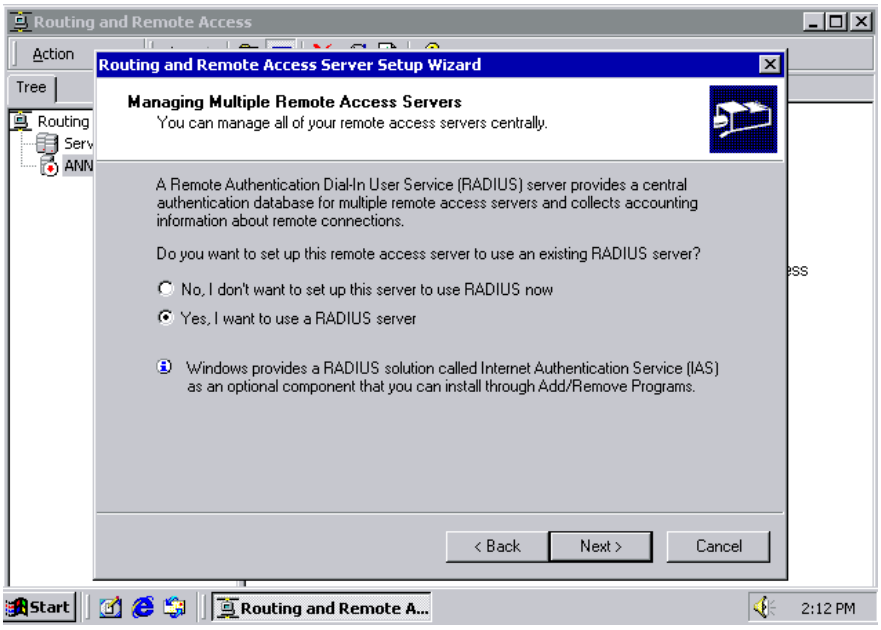

Routing and Remote Access
Action
Tree
Routing
Serv
ANN
Routing and Remote Access Server Setup Wizard
Remote Client Protocols
The protocols required for remote client access must be available on this server.
Verify that the protocols required on this server for remote clients are listed below.
Protocols:
TCP/IP
Yes, all of the required protocols are on this list
No, I need to add protocols
< Back
Next >
Cancel
Start
Routing and Remote A...
2:01 PM

6. Specify your IP address as shown on the following screens:


Routing and Remote Access
Action
Tree
Routing
Serv
ANN
Routing and Remote Access Server Setup Wizard
IP Address Assignment
You can select the method for assigning IP addresses to remote clients.
How do you want IP addresses to be assigned to remote clients?
Automatically
If you use a DHCP server to assign addresses, confirm that it is configured properly.
If you do not use a DHCP server, this server will generate the addresses.
From a specified range of addresses
< Back
Next >
Cancel
Start
Routing and Remote A...
2:03 PM


Routing and Remote Access
Action
Tree
Routing and Remote Access Server Setup Wizard
Address Range Assignment
You can specify the address ranges that this server will use to assign addresses to remote clients.
New Address Range
Type a starting IP address and either an ending IP address or the number of addresses in the range.
Start IP address:
End IP address:
Number of addresses:
OK
Cancel
< Back
Next >
Cancel
Start
Routing and Remote A...
2:05 PM

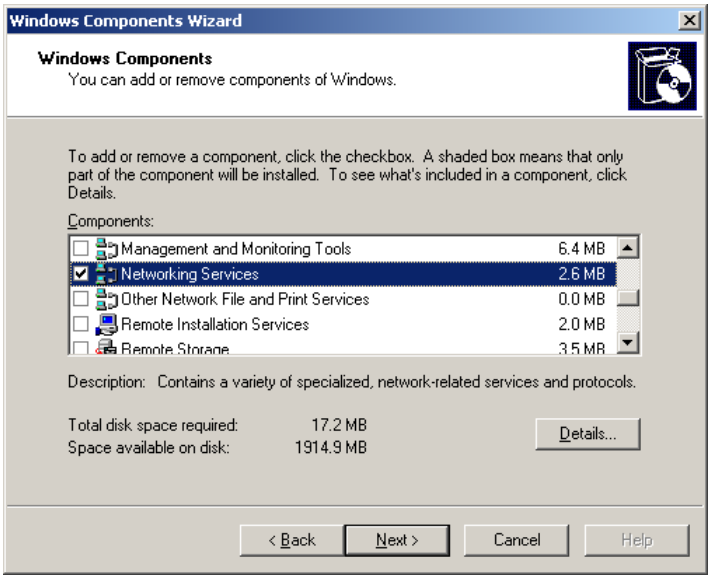
7. Select **Yes**, I want to use a RADIUS server and click **Next**.


Routing and Remote Access
Action
Tree
Routing and Remote Access Server Setup Wizard
Managing Multiple Remote Access Servers
You can manage all of your remote access servers centrally.
A Remote Authentication Dial-In User Service (RADIUS) server provides a central authentication database for multiple remote access servers and collects accounting information about remote connections.
Do you want to set up this remote access server to use an existing RADIUS server?
No, I don't want to set up this server to use RADIUS now
Yes, I want to use a RADIUS server
Windows provides a RADIUS solution called Internet Authentication Service (IAS) as an optional component that you can install through Add/Remove Programs.
< Back
Next >
Cancel
Start
Routing and Remote A...
2:12 PM

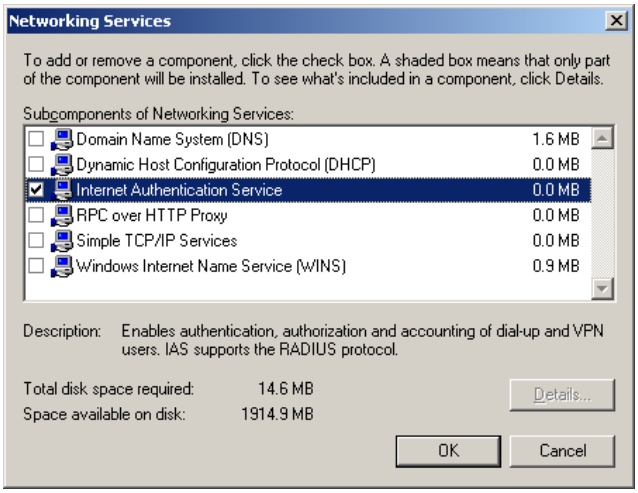
Setting up Windows 2003 Hosts

Windows 2003 uses the IAS service instead of the RADIUS service. For this reason, you need to install the IAS service to use RADIUS with Windows 2003 (The IAS service will not be installed by default).

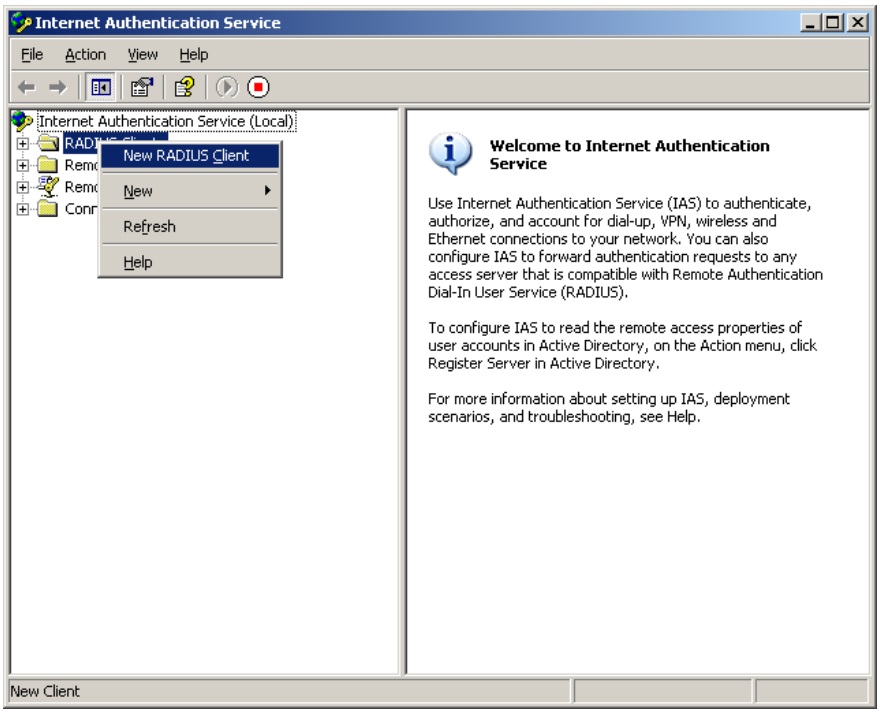
1. Open **Start → Add or Remove Programs → Add/Remove Windows Components.**
2. With **Windows Components** selected, choose **Networking Services**.


Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 6.4 MB
Networking Services 2.6 MB
Other Network File and Print Services 0.0 MB
Remote Installation Services 2.0 MB
Remote Storage 3.5 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 17.2 MB
Space available on disk: 1914.9 MB
Details...
< Back
Next >
Cancel
Help

3. Select **Details**, and then select **Internet Authentication Service**. Continue clicking **OK** until the installation is complete.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Domain Name System (DNS) 1.6 MB
Dynamic Host Configuration Protocol (DHCP) 0.0 MB
Internet Authentication Service 0.0 MB
RPC over HTTP Proxy 0.0 MB
Simple TCP/IP Services 0.0 MB
Windows Internet Name Service (WINS) 0.9 MB
Description: Enables authentication, authorization and accounting of dial-up and VPN users. IAS supports the RADIUS protocol.
Total disk space required: 14.6 MB
Space available on disk: 1914.9 MB
Details...
OK
Cancel

4. After the installation is complete, click **Administrative Tools** and run the **Internet Authentication Service**. This will open the following window.


Internet Authentication Service
File Action View Help
Internet Authentication Service (Local)
New RADIUS Client
New
Refresh
Help
Welcome to Internet Authentication Service
Use Internet Authentication Service (IAS) to authenticate, authorize, and account for dial-up, VPN, wireless and Ethernet connections to your network. You can also configure IAS to forward authentication requests to any access server that is compatible with Remote Authentication Dial-In User Service (RADIUS).
To configure IAS to read the remote access properties of user accounts in Active Directory, on the Action menu, click Register Server in Active Directory.
For more information about setting up IAS, deployment scenarios, and troubleshooting, see Help.
New Client

5. Select **New RADIUS Client** to add a new RADIUS client. You will then be able to begin using this function.